kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 АО "Лаборатория Касперского"

Мазмұны

Kaspersky Security Center 15.1 бағдарламасына анықтама

Не жаңалық

Kaspersky Security Center туралы

- Бағдарлама архитектурасы
- Аппараттық және бағдарламалық талаптар
  - Басқару серверіне қойылатын талаптар
  - Web Console консоліне қойылатын талаптар
  - Ұялы құрылғылар серверіне қойылатын талаптар
  - Басқару консоліне қойылатын талаптар
  - Желілік агентіне қойылатын талаптар
- Kaspersky үйлесімді бағдарламалары мен шешімдері
- Kaspersky Security Center 15.1 лицензиялары мен мүмкіндіктері
- Kaspersky Security Center құрамдастарының үйлесімділігі туралы ақпарат
- Kaspersky Security Center нұсқаларын салыстыру: Windows негізінде және Linux негізінде
- Kaspersky Next Expert View туралы

Kaspersky Security Center 15.1

- Негізгі ұғымдар
  - Басқару сервері
  - Басқару серверлерінің иерархиясы
  - Виртуалды Басқару сервері
  - Ұялы құрылғылардың сервері
  - Веб-сервер
  - Желілік агент
  - Басқару топтары
  - Басқарылатын құрылғы
  - Тағайындалмаған құрылғы
  - Әкімшінің жұмыс станциясы
  - Басқару плагині
  - Басқару веб-плагиндері
  - Саясаттар
  - Саясат профильдері
  - Тапсырмалар
  - Тапсырманың әрекет ету ауқымы
  - Саясат пен бағдарламаның жергілікті параметрлерінің өзара байланысы
  - Тарату нүктесі
  - Қосылым шлюзі
- Негізгі орнату сценарийі
- Kaspersky Security Center қолданатын порттар
- Kaspersky Security Center-мен жұмыс істеуге арналған сертификаттар
  - Kaspersky Security Center сертификаттары туралы
  - Басқару серверінің сертификаты туралы
  - Kaspersky Security Center-де қолданылатын пайдаланушы сертификаттарына қойылатын талаптар
  - Сценарий: Басқару серверінің пайдаланушы сертификатын белгілеу

klsetsrvcert утилитасын пайдаланып, Басқару сервері сертификатын ауыстыру
Желілік агенттерді klmover утилитасын пайдаланып Басқару серверіне қосу
Веб-сервер сертификатын қайта шығару
Деректер трафигі және порттарды пайдалану схемалары
Жергілікті желідегі (LAN) Басқару сервері және басқарылатын құрылғылар
Жергілікті желідегі (LAN) негізгі Басқару сервері және екі қосалқы Басқару сервері
Жергілікті желі (LAN) ішіндегі басқару сервері, интернеттегі басқарылатын құрылғылар; кері прокси-серверді пайдалану
Жергілікті желі (LAN) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар; қосылым шлюзін қолдану
Демилитаризацияланған аймақтың (DMZ) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар
Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларының өзара әрекеттесуі: қосымша мәліметтер
Өзара әрекеттесу схемаларындағы шартты белгілер
Басқару сервері және ДҚБЖ
Басқару сервері және Басқару консолі
Басқару сервері және клиент құрылғысы: Қауіпсіздік бағдарламасын басқару
Тарату нүктесін пайдаланып клиент құрылғысындағы бағдарламалық жасақтаманы жаңарту
Басқару серверлерінің иерархиясы: негізгі Басқару сервері және қосалқы Басқару сервері
Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы
Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы
Басқару сервері және демилитаризацияланған аймағы екі құрылғы: қосылымдар шлюзі және клиент құрылғысы
Басқару сервері және Kaspersky Security Center Web Console
Ұялы құрылғыда қауіпсіздік қолданбасын белсендіру және басқару
Үздік енгізу практикалары
Қорғанысты күшейту нұсқаулығы
Басқару серверін орналастыру
Қосылым қауіпсіздігі
Есептік жазбалар және авторизация
Басқару серверін қорғауды басқару
Клиент құрылғыларын қорғауды басқару
Басқарылатын қолданбалар қорғанысын конфигурациялау
Басқару серверіне техникалық қызмет көрсету
Оқиғаларды үшінші тарап жүйелеріне беру
Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар
Kaspersky қауіпсіздік қолданбаларын пайдалануға қатысты ұсыныстар
Орналастыруға дайындық
Kaspersky Security Center орналастыруды жоспарлау
Қорғаныс жүйесін орналастырудың типтік тәсілдері
Kaspersky Security Center бағдарламасын ұйымның желісінде орналастыруды жоспарлау туралы
Ұйымның қорғаныс құрылымын таңдау
Kaspersky Security Center типтік конфигурациялары
Типтік конфигурация: бір кеңсе
Типтік конфигурация: өзіндік әкімшілері бар бірнеше үлкен кеңсе
Типтік конфигурация: қашықтағы көптеген шағын кеңселер
Басқару сервері үшін ДҚБЖ таңдау
SQL Server 2019 бағдарламасын ДҚБЖ ретінде пайдаланған кезде CU12 жинақталған патчын қолдану
Kaspersky Security Center 15.1 нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы
Kaspersky Security Center 15.1 нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы

Kaspersky Security Center 15.1 бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау
Kaspersky Endpoint Security for Android орнатылған ұялы құрылғыларын басқару
Басқару серверіне интернеттен қатынасуды ұсыну
Интернеттен қатынасу: жергілікті желідегі Басқару сервері
Интернеттен қатынасу: Демилитаризацияланған аймақтағы Басқару сервері
Интернеттен қатынасу: Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану
Тарату нүктелері туралы
klnagent қызметі үшін файл дескрипторларының шектеуін арттыру
Тарату нүктелерінің саны мен конфигурациясын есептеу
Басқару серверлерінің иерархиясы
Виртуалды Басқару серверлері
Kaspersky Security Center шектеулері туралы ақпарат
Желіге түсетін жүктеме
Антивирустық қорғанысты алғашқы рет орналастыру
Антивирустық дерекқорларды алғашқы рет жаңарту
Клиентті Басқару серверімен синхрондау
Антивирустық дерекқорларды қосымша жаңарту
Клиенттердің оқиғаларын Басқару серверінің өңдеуі
Тәулік ішіндегі трафик шығыны
Ұялы құрылғыларды басқаруға дайындық
iOS MDM сервері
Типтік конфигурация: демилитаризацияланған аймақтағы Kaspersky Device Management for iOS
Типтік конфигурация: ұйымның жергілікті желісіндегі iOS MDM сервері
Kaspersky Endpoint Security for Android орнатылған ұялы құрылғыларын басқару
Басқару серверінің өнімділігі туралы мәліметтер
Басқару серверіне қосылу шектеулері
Басқару серверінің өнімділігін тестілеу нәтижелері
KSN прокси-серверінің өнімділігін тексеру нәтижелері
Сыртқы қызметтермен әрекеттесуге арналған желі параметрлері
Желілік агент пен қауіпсіздік бағдарламасын орналастыру
Бастапқы орналастыру
Инсталляторлар параметрлерін конфигурациялау
Орнату пакеттері
MSI сипаттары және түрлендіру файлдары
Қолданбаларды қашықтан орнатудың үшінші тарап құралдары арқылы орналастыру
Kaspersky Security Center бағдарламаларын қашықтан орнату тапсырмалары туралы
Құрылғының бейнесін қармау және көшіру арқылы енгізу
Қатты дискінің кескіні дұрыс көшірілмеді
Microsoft Windows топтық саясаттары тетігінің көмегімен орналастыру
Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру
Kaspersky Security Center қалыптастырған автономды пакеттерді іске қосу
Қолданбаларды қолмен басқару мүмкіндіктері
MST файлын құру
Желілік агенті орнатылған құрылғыларға бағдарламаларды қашықтан орнату
Қашықтан орнату тапсырмасында құрылғыларды қайта жүктеуді басқару
Қауіпсіздік бағдарламасының орнату пакетіндегі дерекқорларды жаңартудың орындылығы

Ерікті орындалатын файлдардың басқарылатын құрылғыларында іске қосу үшін Kaspersky Security Center қолданбаларын қашықтан орнату құралдарын қолдану
Орналастыру мониторингі
Инсталляторлар параметрлерін конфигурациялау
Жалпы ақпарат
Тыныш режимде орнату (жауаптар файлымен)
Желілік агентті тыныш режимде орнату (жауаптар файлы жоқ)
setup.exe арқылы орнату параметрлерін ішінара конфигурациялау
Басқару серверін орнату параметрлері
Желілік агентті орнату параметрлері
Виртуалды инфрақұрылым
Виртуалды машиналарға түсетін жүктемені азайту бойынша ұсынымдар
Динамикалық виртуалды машиналарды қолдау
Виртуалды машиналарды көшіруді қолдау
Желілік агенті бар құрылғылар үшін файлдық жүйені шегіндіруді қолдау
Бағдарламаларды жергілікті түрде орнату
Желілік агентті жергілікті орнату
Желілік агентті тыныш режимде орнату
Linux үшін Желілік агентті тыныш режимде орнату (жауап файлымен)
Желілік агентті орнату үшін жабық бағдарлама ортасы режимінде Astra Linux басқаратын құрылғыны дайындау
Linux үшін Желілік агентті интерактивті режимде орнату
Бағдарламаны басқару плагинін жергілікті түрде орнату
Бағдарламаларды тыныш режимде орнату
Бағдарламаларды автономды пакеттердің көмегімен орнату
Желілік агенттің орнату пакетінің параметрлері
Құпиялылық саясатын қарау
Ұялы құрылғыларды басқару жүйелерін орналастыру
iOS MDM протоколы бойынша басқару жүйесін орналастыру
iOS MDM серверін орнату
iOS MDM серверін тыныш режимде орнату
iOS MDM серверін орналастыру схемалары
Жеңілдетілген орналастыру схемасы
Kerberos Constrained Delegation (KCD) мәжбүрлеп табыстауын қолдана отырып орналастыру схемасы
APNs сертификатын алу
APNs сертификатын жаңарту
iOS MDM серверінің резервтік сертификатын конфигурациялау
APNs сертификатын iOS MDM серверіне орнату
Apple Push Notification сервисіне қатынасты конфигурациялау
Ұялы құрылғыға жалпы сертификат беру және орнату
KES құрылғысын басқарылатын құрылғылар тізіміне қосу
KES құрылғыларын Басқару серверіне қосу
Құрылғыларды Басқару серверіне тікелей қосу
Kerberos (KCD) мәжбүрлеп табыстау арқылы KES құрылғыларын Серверге қосу схемасы
Firebase Cloud Messaging қолдану
Жалпыға ортақ кілттер инфрақұрылымымен біріктіру
Kaspersky Security Center Web Server

Kaspersky Security Center орнату
Орнатуға дайындық
ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар
SQL Server серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау (Windows түпнұсқалық растамасы)
SQL Server серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау (SQL Server түпнұсқалық растамасы)
MySQL және MariaDB жүйесімен жұмыс істеу үшін есептік жазбаларды конфигурациялау
Деректерді MySQL және MariaDB ДҚБЖ-лардағы ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу
PostgreSQL және Postgres Pro жүйесімен жұмыс істеу үшін есептік жазбаларды конфигурациялау
Microsoft SQL Server түпнұсқалық растамасы
Сценарий: MySQL Server серверінің аутентификациясы
Сценарий: PostgreSQL Server серверінің аутентификациясы
Басқару серверін орнату бойынша ұсыныстар
Істен шығуға төзімді кластерде Басқару серверінің қызметтеріне арналған есептік жазбалар жасау
Ортақ қатынасы бар қалтаны белгілеу
Active Directory топтық саясаттары көмегімен Басқару серверінің құралдарымен қашықтағы орнату
Автономды пакетке UNC-жолын тарату арқылы қашықтан орнату
Басқару серверінің ортақ қатынасы бар қалтасынан жаңарту
Операциялық жүйенің кескіндерін орнату
Басқару серверінің мекенжайын көрсету
Стандартты орнату
1-қадам. Лицензиялық келісім мен Құпиялық саясатын қарап шығу
2-қадам. Орнату түрі таңдау
3-қадам. Kaspersky Security Center Web Console орнату
4-қадам. Желінің өлшемін таңдау
5-қадам. Дерекқорды таңдау
6-қадам. SQL сервері параметрлерін конфигурациялау
7-қадам. Түпнұсқалық растама режимін таңдау
8-қадам. Файлдарды мұрағаттан шығарып, қатты дискіге орнату
Таңдаулы орнату
1-қадам. Лицензиялық келісім мен Құпиялық саясатын қарап шығу
2-қадам. Орнату түрі таңдау
3-қадам. Орнату үшін құрамдастарды таңдау
4-қадам. Kaspersky Security Center Web Console орнату
5-қадам. Желінің өлшемін таңдау
6-қадам. Дерекқорды таңдау
7-қадам. SQL сервері параметрлерін конфигурациялау
8-қадам. Түпнұсқалық растама режимін таңдау
9-қадам. Басқару серверін іске қосу үшін есептік жазбаны таңдау
10-қадам. Kaspersky Security Center қызметтерін іске қосу үшін есептік жазбаны таңдау
11-қадам. Ортақ қатынасы бар қалтаны анықтау
12-қадам. Басқару серверіне қосылу параметрлерін конфигурациялау
13-қадам. Басқару сервері мекенжайын белгілеу
14-қадам. Ұялы құрылғыларды қосу үшін Сервер мекенжайы
15-қадам. Бағдарламаларды басқару плагиндерін таңдау
16-қадам. Файлдарды мұрағаттан шығарып, қатты дискіге орнату

Ақауларға төзімді Kaspersky Security Center кластерін орналастыру
Сценарий: Kaspersky Security Center ақауларға төзімді кластерін орналастыру
Ақауларға төзімді Kaspersky Security Center кластері туралы ақпарат
Ақауларға төзімді Kaspersky Security Center кластері үшін файлдық серверді дайындау
Ақауларға төзімді Kaspersky Security Center кластері үшін түйіндерді дайындау
Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйіндеріне орнату
Кластер түйінін қолмен іске қосу және тоқтату
Басқару серверін ақауларға төзімді Windows Server кластеріне орнату
1-қадам. Лицензиялық келісім мен Құпиялық саясатын қарап шығу
2-қадам. Кластерге орнату түрін таңдау
3-қадам. Виртуалды Басқару сервері атауын көрсету
4-қадам. Виртуалды Басқару сервері желісінің параметрлерін көрсету
5-қадам. Кластерлер тобын көрсету
6-қадам. Кластерлік деректер қоймасын таңдау
7-қадам. Қашықтан орнату үшін есептік жазбаны көрсету
8-қадам. Орнату үшін құрамдастарды таңдау
9-қадам. Желінің өлшемін таңдау
10-қадам. Дерекқорды таңдау
11-қадам. SQL сервері параметрлерін конфигурациялау
12-қадам. Түпнұсқалық растама режимін таңдау
13-қадам. Басқару серверін іске қосу үшін есептік жазбаны таңдау
14-қадам. Kaspersky Security Center қызметтерін іске қосу үшін есептік жазбаны таңдау
15-қадам. Ортақ қатынасы бар қалтаны анықтау
16-қадам. Басқару серверіне қосылу параметрлерін конфигурациялау
17-қадам. Басқару сервері мекенжайын белгілеу
18-қадам. Ұялы құрылғыларды қосу үшін Сервер мекенжайы
19-қадам. Файлдарды мұрағаттан шығарып, қатты дискіге орнату
Басқару серверін тыныш режимде орнату
Басқару консолін әкімшінің жұмыс орнына орнату
Kaspersky Security Center орнатқаннан кейін жүйеде орын алған өзгерістер
Бағдарламаны жою
Kaspersky Security Center алдыңғы нұсқасын жаңарту туралы
Kaspersky Security Center алдыңғы нұсқасын жаңарту
Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйінінде жаңарту
Ақауларға төзімді Microsoft кластер түйіндеріндегі Kaspersky Security Center орталығын жаңарту
Kaspersky Security Center бастапқы конфигурациялау
Қорғанысты күшейту нұсқаулығы
Басқару серверін жылдам іске қосу шебері
Бағдарламаны жылдам іске қосу шебері туралы
Басқару серверін жылдам іске қосу шеберін іске қосу
1-қадам. Прокси-сервер параметрлерін конфигурациялау
2-қадам. Бағдарламаны белсендіру тәсілін таңдау
3-қадам. Қорғаныс аумағы мен операциялық жүйелерді таңдау
4-қадам. Басқарылатын бағдарламаларға арналған плагиндерді таңдау
5-қадам. Дистрибутивтерді жүктеу және орнату пакеттерін жасау
6-қадам. Kaspersky Security Network қолдануды конфигурациялау

7-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау
8-қадам. Жаңартуларды басқару параметрлерін конфигурациялау
9-қадам. Қорғаудың бастапқы конфигурациясын жасау
10-қадам. Ұялы құрылғыларды қосу
11-қадам. Жаңартуларды жүктеп алу
12-қадам. Құрылғыларды табу
13-қадам. Бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау
Басқару консолі мен Басқару серверінің қосылымын конфигурациялау
Басқару серверінің интернетке қатынасу параметрлерін конфигурациялау
Автономды құрылғыларды қосу
Сценарий: Автономды құрылғыларды қосылым шлюзі арқылы қосу
Сценарий: демилитаризацияланған аймақтағы Басқару сервері арқылы автономды құрылғыларды қосу
Автономды құрылғыларды қосу туралы
Сыртқы компьютер құрылғыларын басқару серверіне қосу
Автономды пайдаланушыларға арналған қосылым профильдері туралы
Автономды пайдаланушылар үшін қосылым профилін жасау
Желілік агентті басқа Басқару серверіне ауыстырып қосу туралы
Желілік агентті желілік орналасу бойынша ауыстырып қосу ережесін жасау
Оқиға хабарландырулары
Оқиға хабарландырулары параметрлерін конфигурациялау
Хабарландыруларды таратуды тексеру
Орындалатын файл көмегімен оқиғалар туралы хабарлау
TLS қосылымын шифрлау
Интерфейсті конфигурациялау
Желідегі құрылғыларды табу
Сценарий: Желілік құрылғыларды табу
Тағайындалмаған құрылғылар
Құрылғыларды табу
Windows желісінің сауалнамасы
Active Directory сауалнамасы
IP ауқымдарының сауалнамасы
Zeroconf сауалнамасы
Windows домендерімен жұмыс істеу. Домен параметрлерін көру және өзгерту
Тағайындалмаған құрылғылар үшін сақтау ережелерін конфигурациялау
IP ауқымдарымен жұмыс істеу
IP ауқымын жасау
IP ауқымдары параметрлерін көру және өзгерту
Active Directory топтарымен жұмыс істеу Топ параметрлерін қарап шығу және өзгерту
Құрылғыларды басқару топтарына автоматты түрде жылжыту ережелерін құру
Клиент құрылғыларында VDI динамикалық режимін пайдалану
Желілік агенттің орнату пакетінің сипаттарында VDI динамикалық режимін қосу
VDI құрамына кіретін құрылғыларды табу
VDI құрамына кіретін құрылғыларды басқару тобына жылжыту
Жабдықты түгендеу
Жаңа құрылғылар туралы ақпаратты қосу
Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау
Пайдаланушы өрістерін конфигурациялау

Бағдарламаны лицензиялау
Лицензия шектеуден асып кету оқиғалары
Лицензиялау туралы
Лицензия туралы
Лицензиялық келісім туралы
Лицензиялық сертификат туралы
Лицензиялық кілт туралы
Кілт файлы туралы
Жазылым туралы
Белсендіру коды туралы
Лицензиялық келісімге берілген келісімді кері қайтарып алу
Деректерді беру туралы
Kaspersky Security Center лицензиялау нұсқалары
Kaspersky Security Center және басқарылатын бағдарламаларды лицензиялау ерекшеліктері
Kaspersky бағдарламалары. Орталықтандырылған орналастыру
Үшінші тарап қауіпсіздік бағдарламаларын алмастыру
Қашықтан орнату тапсырмасын пайдаланып бағдарламаларды орнату
Бағдарламаны таңдалған құрылғыларға орнату
Бағдарламаны басқару тобының клиент құрылғыларына орнату
Active Directory топтық саясаты арқылы бағдарламаны орнату
Қолданбаларды macOS құрылғыларына қашықтан орнату
Қосалқы Басқару серверлеріне бағдарламаларды орнату
Қашықтан орнату шеберін пайдаланып бағдарламаларды орнату
Басқару плагиндерімен жұмыс істеу
Қорғаныс орналастыру туралы есепті қарап шығу
Бағдарламаларды қашықтан жою
Басқару тобының клиент құрылғыларынан бағдарламаны қашықтан жою
Таңдалған құрылғылардан бағдарламаны қашықтан жою
Орнату пакеттерімен жұмыс істеу
Орнату пакетін жасау
Автономды орнату пакетін жасау
Пайдаланушы орнату пакетін жасау
Пайдаланушы орнату пакеттерінің сипаттарын қарап шығу және өзгерту
Kaspersky Security Center жеткізу жиынтығындағы Желілік агенттің орнату пакетін алу
Орнату пакеттерін қосалқы Басқару серверлеріне тарату
Орнату пакеттерін тарату нүктелері көмегімен тарату
Kaspersky Security Center-ге бағдарламаны орнату нәтижелері туралы ақпаратты жіберу
Орнату пакеттері үшін KSN прокси-сервері мекенжайын анықтау
Бағдарламалардың өзекті нұсқаларын алу
Windows басқаратын құрылғыны қашықтан орнатуға дайындау
Linux операциялық жүйесімен жұмыс істейтін құрылғыны дайындау және Linux операциялық жүйесі бар құрылғыға Желілік агентті қашықтан орнату
SUSE Linux Enterprise Server 15 басқаратын құрылғыны Желілік агентті орнатуға дайындау
macOS операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау
Kaspersky бағдарламасы: лицензиялау және белсендіру
Басқарылатын бағдарламаларды лицензиялау
Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу

Лицензиялық кілтті Басқару серверінің қоймасына қосу
Басқару серверінің лицензия кілтін өшіру
Лицензиялық кілтті клиент құрылғыларына тарату
Лицензиялық кілтті автоматты түрде тарату
Лицензиялық кілттерді қолдану туралы есепті жасау және қарап шығу
Бағдарламаның лицензиялық кілттері туралы ақпаратты қарап шығу
Кілт файлын экспорттау
Желі қорғанысын конфигурациялау
Сценарий: Желі қорғанысын конфигурациялау
Саясаттарды конфигурациялау және тарату: құрылғыларға бағытталған тәсілдеме
Құрылғыларға және пайдаланушыларға бағытталған қауіпсіздікті басқару тәсілдемелері
Kaspersky Endpoint Security саясатын қолмен конфигурациялау
Кеңейтілген қорғаныс бөлімінде саясатты конфигурациялау
Негізгі қорғаныс бөліміндегі саясатты конфигурациялау
Қосымша параметрлер бөліміндегі саясатты конфигурациялау
Оқиғаларды конфигурациялау бөліміндегі саясатты конфигурациялау
Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау
Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау
Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау
Жаңартуларды орнату және осалдықты түзету топтық тапсырмасын қолмен конфигурациялау
Оқиғалар қоймасындағы оқиғалар санын конфигурациялау
Түзетілген осалдықтар туралы ақпаратты сақтаудың максималды мерзімін белгілеу
Тапсырмаларды басқару
Тапсырманы жасау
Басқару серверінің тапсырмасын жасау
Арнайы құрылғыларға арналған тапсырмалар жасау
Жергілікті тапсырма жасау
Салынған топтың жұмыс аймағында иеленген топтық тапсырманы көрсету
Тапсырманы іске қоспас бұрын құрылғыларды автоматты түрде қосу
Тапсырманы орындағаннан кейін құрылғыны автоматты түрде өшіру
Тапсырманы орындау уақытын шектеу
Тапсырманы экспорттау
Тапсырманы импорттау
Тапсырмаларды түрлендіру
Тапсырманы қолмен іске қосу және тоқтату
Тапсырманы қолмен тоқтата тұру және жалғастыру
Тапсырманы орындау барысын бақылау
Басқару серверінде сақталатын тапсырмаларды орындау нәтижелерін қарап шығу
Тапсырманы орындау нәтижелері туралы ақпарат сүзгісін конфигурациялау
Тапсырманы өзгерту. Өзгерістерді шегіндіру
Тапсырмаларды салыстыру
Тапсырмаларды іске қосуға арналған есептік жазбалар
Тапсырманы орындау тарихын экспорттау
Тапсырмалардың құпиясөзін өзгерту шебері
1-қадам. Есептік деректерді таңдау
2-қадам. Орындалып жатқан әрекетті таңдау
3-қадам. Нәтижелерді қарап шығу

- Виртуалды Басқару серверіне бағынатын басқару топтары иерархиясын жасау
- Саясаттар және профильдер
  - Саясаттар иерархиясы, саясат профильдерін қолдану
    - Саясаттар иерархиясы
    - Саясат профильдері
    - Саясат параметрлерін иелену
  - Саясатты басқару
    - Саясатты жасау
    - Салынған топта иеленген саясатты көрсету
    - Саясатты белсендіру
    - "Вирустық шабуыл" оқиғасы бойынша саясатты автоматты түрде белсендіру
    - Автономды пайдаланушылар саясатын қолдану
    - Саясатты өзгерту. Өзгерістерді шегіндіру
    - Саясаттарды салыстыру
    - Саясатты қолдану күйінің диаграммасын қарау
    - Саясатты жою
    - Саясатты көшіру
    - Саясатты экспорттау
    - Саясатты импорттау
    - Саясаттарды түрлендіру
  - Саясат профильдерін басқару
    - Саясат профилін жасау
    - Саясат профилін өзгерту
    - Саясат профилін жою
    - Саясатын профилін белсендіру ережесін жасау
- Құрылғыны жылжыту ережелері
- Құрылғыны жылжыту ережелерін көшіру
- Бағдарламалық жасақтаманы санаттау
- Бағдарламаларды ұйым-клиент құрылғыларына орнату үшін қажетті шарттар
- Бағдарламаның жергілікті параметрлерін көру және өзгерту

Kaspersky Security Center және басқарылатын бағдарламаларды жаңарту

- Сценарий: Kaspersky бағдарламалары мен дерекқорларын үнемі жаңартып тұру
- Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту туралы
- Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану туралы
- Айырмашылық файлдарын жүктеу функциясын қосу
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау
- Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау
- Жаңартуларды Басқару серверінің сақтау орнына жүктеу тапсырмасының параметрлерін конфигурациялау
- Алынған жаңартуларды тексеру
- Тексеру саясаттары мен көмекші тапсырмаларды конфигурациялау
- Алынған жаңартуларды қарап шығу
- Құрылғыларға Kaspersky Endpoint Security жаңартуларын автоматты түрде орнату
- Жаңартуларды алудың офлайн-моделі
- Жаңартуларды алудың офлайн-моделін қосу және өшіру
- Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнату
- Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру

- Жаңартуларды автоматты түрде тарату
  - Жаңартуларды клиент құрылғыларына автоматты түрде тарату
  - Жаңартуларды қосалқы Басқару серверлеріне автоматты түрде тарату
  - Тарату нүктелерін автоматты түрде тағайындау
  - Құрылғыны қолмен тарату нүктесі етіп тағайындау
  - Құрылғыны тарату нүктелері тізімінен алып тастау
  - Тарату нүктелері арқылы жаңартуларды жүктеп алу
- Қоймадан бағдарламалық жасақтама жаңартуларын жою
- Кластерлік модельде Kaspersky бағдарламасына арналған патч орнату

Клиент құрылғыларындағы үшінші тарап бағдарламалары бағдарламаларын басқару

- Үшінші тарап бағдарламалары туралы
- Үшінші тарап бағдарламаларының жаңартуларын орнату
  - Сценарий: Үшінші тарап бағдарламаларын жаңарту
  - Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау
  - Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
  - Windows Update жаңартуларын Басқару серверімен синхрондау
    - 1-қадам. Трафикті азайту қажеттілігін анықтау
    - 2-қадам. Бағдарламалар
    - 3-қадам. Жаңартулар санаттары
    - 4-қадам. Жаңартулардың локализация тілі
    - 5-қадам. Тапсырманы іске қосу үшін есептік жазбаны таңдау
    - 6-қадам. Тапсырма кестесін конфигурациялау
    - 7-қадам. Тапсырманың атауын анықтау
    - 8-қадам. Тапсырманы жасауды аяқтау
  - Құрылғыларға жаңартуларды қолмен орнату
  - Желілік агент саясатында Windows жаңартуларын конфигурациялау
- Үшінші тарап қолданбаларында осалдықтарды түзету
  - Сценарий: Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету
  - Бағдарламалық жасақтама осалдықтарын анықтау және түзету туралы
  - Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау
  - Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау
  - Бағдарламалық жасақтама осалдықтарын іздеу
  - Бағдарламаларда осалдықты түзету
  - Оқшауланған желіде осалдықтарды түзету
    - Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету
    - Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету туралы
    - Оқшауланған желідегі осалдықтарды түзету үшін интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау
    - Оқшауланған желідегі осалдықтарды түзету үшін оқшауланған Басқару серверлерін конфигурациялау
    - Оқшауланған желіде түзетулерді беру және жаңартуларды орнату
    - Оқшауланған желіде түзетулерді жіберу және жаңартуларды орнату мүмкіндігін өшіру
  - Бағдарламалардағы осалдықтарды елемеу
  - Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушы түзетулері
  - Жаңартулар орнату ережелері
- Бағдарламалар топтары
  - Орындалатын файлдарды басқару үшін Бағдарламаларды басқару компонентін пайдалану
  - Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау

- Kaspersky Endpoint Security для Windows саясаты үшін бағдарлама санаттарын жасау
- Қолмен толықтырылатын бағдарламалар санатын жасау
- Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау
- Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау
- Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу
- Клиент құрылғыларында бағдарламалардың іске қосылуын басқаруды конфигурациялау
- Орындалатын файлдарды іске қосу ережелерін статикалық талдау нәтижелерін қарау
- Бағдарламалар тізімдемелерін қарап шығу
- Бағдарламалық жасақтаманы түгендеудің басталу уақытын өзгерту
- Лицензиялы бағдарламаларда лицензиялық кілттерді басқару туралы
- Лицензиялы бағдарламалар тобын жасау
- Лицензиялы бағдарламалар топтары үшін лицензиялық кілттерді басқару
- Орындалатын файлдарды түгендеу
- Орындалатын файлдар туралы ақпаратты қарау

Бақылау және есеп беру

- Сценарий: Бақылау және есеп беру
- Басқару консолінде түс индикаторлары мен тіркелген оқиғаларды мониторингтеу
- Есептер, статистика және хабарландырулармен жұмыс
  - Есептермен жұмыс
    - Есеп үлгісін жасау
    - Есеп үлгісінің сипаттарын қарау және өзгерту
    - Есеп үлгілеріндегі кеңейтілген сүзгі пішімі
      - Сүзгіні кеңейтілген пішімге түрлендіру
      - Кеңейтілген сүзгіні конфигурациялау
    - Есепті жасау және қарау
    - Есепті сақтау
    - Есептерді жеткізу тапсырмасын жасау
      - 1-қадам. Тапсырма түрін таңдау
      - 2-қадам. Есеп түрін таңдау
      - 3-қадам. Есеппен жасалатын әрекеттер
      - 4-қадам. Тапсырманы іске қосу үшін есептік жазбаны таңдау
      - 5-қадам. Тапсырма кестесін конфигурациялау
      - 6-қадам. Тапсырманың атауын анықтау
      - 7-қадам. Тапсырманы жасауды аяқтау
  - Статистикалық ақпаратпен жұмыс
  - Оқиға хабарландырулары параметрлерін конфигурациялау
  - SMTP сервері үшін сертификат жасау
  - Оқиғалар таңдау
    - Оқиғалар таңдауын қарап шығу
    - Оқиғалар таңдау параметрлерін конфигурациялау
    - Оқиғалар таңдауын жасау
    - Оқиғалар таңдауын мәтіндік файлға экспорттау
    - Оқиғаларды таңдаудан жою
    - Бағдарламаларды пайдаланушылардың сұраулары бойынша ерекшеліктерге қосу
  - Құрылғыны таңдаулары
    - Құрылғы таңдауларын қарап шығу
    - Құрылғы таңдауларын конфигурациялау

Құрылғы таңдаулары параметрлерін файлға экспорттау
Құрылғы таңдауларын жасау
Импортталған параметрлер бойынша құрылғылар таңдауын жасау
Таңдаудағы басқару топтарынан құрылғыларды жою
Бағдарламаларды орнату және жою мониторингі
Kaspersky Security Center құрамдастарының оқиғалары
Оқиға түрі сипаттамасы деректерінің құрылымы
Басқару сервері оқиғалары
Басқару серверінің критикалық оқиғалары
Басқару серверінің функционалдық ақауы оқиғалары
Басқару серверінің ескерту оқиғалары
Басқару серверінің ақпараттық оқиғалары
Желілік агент оқиғалары
Желілік агенттің функционалдық ақауы оқиғалары
Желілік агенттің ескертулері оқиғалары
Желілік агенттің ақпараттық оқиғалары
iOS MDM сервері оқиғалары
iOS MDM серверінің функционалдық ақауы оқиғалары
iOS MDM серверінің ескерту оқиғалары
iOS MDM серверінің ақпараттық оқиғалары
Жиі болатын оқиғаларды бұғаттау
Жиі болатын оқиғаларды бұғаттау туралы
Жиі болатын оқиғаларды бұғаттауды басқару
Жиі болатын оқиғады бұғаттауды болдырмау
Жиі болатын оқиғалар тізімін файлға экспорттау
Виртуалды машиналардың күйінің өзгеруін бақылау
Жүйелік тізімдемедегі ақпарат арқылы антивирустық қорғаныс күйін бақылау
Құрылғы белсенді емес кезде әрекеттерді қарау және конфигурациялау
Kaspersky хабарландыруларын өшіру
Тарату нүктелері мен қосылым шлюздерін конфигурациялау
Тарату нүктелерінің типтік конфигурациясы: бір кеңсе
Тарату нүктелерінің типтік конфигурациясы: қашықтағы көптеген шағын кеңселер
Басқарылатын құрылғыны тарату нүктесі етіп тағайындау
Linux жүйесінде жұмыс істейтін құрылғыны демилитаризацияланған аймақта шлюз ретінде қосу
Linux жүйесінде жұмыс істейтін құрылғыны қосылым шлюзі арқылы Басқару серверіне қосу
Қосылым шлюзін тарату нүктесі ретінде демилитаризацияланған аймаққа қосу
Тарату нүктелерін автоматты түрде тағайындау
Тарату нүктесі таңдаған құрылғыға Желілік агентті жергілікті орнату туралы
Тарату нүктесін қосылым шлюзі ретінде қолдану туралы
Тарату нүктесі сұралатын ауқымдар тізіміне IP ауқымдарын қосу
Тарату нүктесін хабарлаушы сервер ретінде қолдану
Басқа да күнделікті тапсырмалар
Басқару серверлерін басқару
Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу
Басқару серверіне қосылу және Басқару серверлері арасында ауысу
Басқару серверіне және оның нысандарына қатынасу құқықтары
Басқару серверіне интернет арқылы қосылу шарттары

- Басқару серверіне қорғалған қосылым
  - Құрылғыны қосу кезіндегі Сервердің түпнұсқалық растамасы
  - Басқару консолін қосу кезінде Сервердің түпнұсқалық растамасы
- Басқару серверіне қосылуға арналған рұқсат етілген IP мекенжайлары тізімін конфигурациялау
- 13291-портты жабу үшін klscflag утилитасын пайдалану
- Басқару серверінен ажырау
- Консоль ағашына Басқару серверін қосу
- Консоль ағашынан Басқару серверін жою
- Консоль шежіресіне виртуалды Басқару серверін қосу
- Басқару сервері қызметінің есептік жазбасын ауыстыру. klsrvswch утилитасы
- ДҚБЖ есептік деректерін өзгерту
- Басқару серверінің ортақ қатынасы бар қалтасын өзгерту
- Басқару сервері түйіндерінің мәселелерін шешу
- Басқару сервері параметрлерін қарау және өзгерту
  - Басқару серверінің жалпы параметрлерін көрсету
  - Басқару консолі интерфейсінің параметрлері
  - Басқару серверінде оқиғаларды өңдеу және сақтау
  - Басқару серверіне Қосылымдар журналдарын қарау
  - Вирустық індеттердің туындауын бақылау
  - Трафикті шектеу
  - Веб-сервер параметрлерін конфигурациялау
  - Ішкі пайдаланушылармен жұмыс істеу
- Басқару сервері параметрлерін сақтық көшірмелеу және қалпына келтіру
  - Сақтық көшірмелеу уақытын азайту үшін файлдық жүйенің суретін пайдалану
  - Басқару сервері бар құрылғы істен шықты
  - Басқару серверінің параметрлері немесе дерекқор зақымдалған
- Басқару сервері деректерін сақтық көшірмелеу және қалпына келтіру
  - Басқару сервері деректерін сақтық көшірмелеу тапсырмасы
  - Деректерді сақтық көшірмелеу және қалпына келтіру утилитасы (klbackup)
  - Деректерді интерактивті режимде сақтық көшірмелеу және қалпына келтіру
  - Деректерді тыныш режимде сақтық көшірмелеу және қалпына келтіру
  - Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану
  - MySQL немесе MariaDB пайдалану кезінде басқару сервері деректерінің сақтық көшірмесін жасау және қалпына келтіру
  - Басқару сервері деректерінің сақтық көшірмесін жасау мен қалпына келтіруді оңтайландыру
- Басқару серверін басқа құрылғыға тасымалдау
- Басқару серверлері арасындағы қақтығыстардан аулақ болу

Басқару топтарын басқару

- Басқару топтарын жасау
- Басқару топтарын жылжыту
- Басқару топтарын жою
- Басқару топтарының құрылымын автоматты түрде жасау
- Бағдарламаларды басқару тобының құрылғыларына автоматты түрде орнату

Клиент құрылғыларын басқару

- Клиент құрылғыларын Басқару серверіне қосу
- Клиент құрылғысын Басқару серверіне қолмен қосу. klmover утилитасы

Клиент құрылғысы мен Басқару сервері арасындағы қосылымды туннельдеу
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу
Windows операциялық жүйесі орнатылған клиент құрылғыларына қосылу
macOS операциялық жүйесі орнатылған клиент құрылғыларына қосылу
Windows компьютерлік бөлісу қызметі арқылы құрылғыларға қосылу
Клиент құрылғысын қайта іске қосуды конфигурациялау
Қашықтағы клиент құрылғысындағы әрекеттер аудиті
Клиент құрылғысы мен Басқару сервері арасындағы қосылымды тексеру
Клиент құрылғысы мен Басқару серверінің арасындағы қосылымды автоматты түрде тексеру
Клиент құрылғысы мен Басқару серверінің арасындағы қосылымды қолмен тексеру. klnagchk утилитасы
Құрылғыны Басқару серверіне қосу уақытын тексеру туралы
Басқару серверіндегі клиент құрылғыларын сәйкестендіру
Құрылғыларды басқару тобының құрамына жылжыту
Клиент құрылғылары үшін Басқару серверін ауыстыру
Басқа Басқару серверіне қосылу шлюздері арқылы Басқару серверіне қосылған құрылғыларды жылжыту
Кластерлер және серверлердің массивтері
Клиент құрылғыларын қашықтан қосу, өшіру және қайта іске қосу
Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты қосылымды пайдалану туралы
Мәжбүрлеп синхрондау туралы
Байланыс кестесі туралы
Құрылғылардың пайдаланушыларына хабар жіберу
Kaspersky Security for Virtualization бағдарламасымен жұмыс істеу
Құрылғылардың күйлерін ауыстыруды конфигурациялау
Құрылғыларға тегтерді тағайындау және тағайындалған тегтерді қарап шығу
Құрылғыларға тегтерді автоматты түрде тағайындау
Құрылғыға тағайындалған тегтерді қарап шығу және конфигурациялау
Клиент құрылғыларын қашықтан диагностикалау. Kaspersky Security Center қашықтан диагностикалау утилитасы
Қашықтан диагностикалау утилитасын клиент құрылғысына қосу
Бағдарламадан алынған қоқыс файлын жасау
Трассалауды қосу және өшіру, трассалау файлын жүктеу
Бағдарламалар параметрлерін жүктеу
Оқиғалар журналдарын жүктеу
Бірнеше диагностикалық ақпараттық элементтерді жүктеу
Диагностиканы іске қосу және оның нәтижелерін жүктеу
Бағдарламаларды іске қосу, тоқтату және қайта іске қосу
UEFI деңгейлі қорғанысты құрылғылар
Басқарылатын құрылғының параметрлері
Саясаттардың жалпы параметрлері
Желілік агент саясатының параметрлері
Пайдаланушы есептік жазбаларын басқару
Пайдаланушы есептік жазбаларымен жұмыс
Ішкі пайдаланушының есептік жазбасын қосу
Ішкі пайдаланушының есептік жазбасын өзгерту
Құпиясөзді енгізу әрекеттерінің санын өзгерту
Ішкі пайдаланушы атының бірегейлігін тексеруді конфигурациялау
Қауіпсіздік топтарын қосу
Пайдаланушыны топқа қосу

Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау. Рөлге негізделген қатынасуды басқару
Бағдарлама функцияларына қатынасу құқықтары
Алдын ала анықталған пайдаланушы рөлдері
Пайдаланушы рөлін қосу
Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау
Пайдаланушыларға немесе пайдаланушылар топтарына құқықтарды тағайындау
Қосалқы Басқару серверлеріне пайдаланушы рөлдерін тарату
Пайдаланушыны құрылғының иесі етіп тағайындау
Пайдаланушыларға хабарлар жіберу
Пайдаланушының ұялы құрылғылар тізімін қарау
Пайдаланушыға сертификатты орнату
Пайдаланушыға жазылған сертификаттар тізімін қарау
Виртуалды Басқару сервері әкімшісі туралы
Операциялық жүйелер мен бағдарламаларды қашықтан орнату
Операциялық жүйенің кескіндерін жасау
Операциялық жүйенің кескіндерін орнату
KSN прокси-сервері мекенжайын конфигурациялау
Windows жүйесін алдын ала орнату ортасының драйверлерін (WinPE) қосу
Драйверлерді операциялық жүйенің кескінімен орнату пакетіне қосу
sysprep.exe утилитасы параметрлерін конфигурациялау
Операциялық жүйелерді желідегі жаңа құрылғыларға орналастыру
Клиент құрылғыларында операциялық жүйелерді орналастыру
Бағдарламалардың орнату пакеттерін жасау
Бағдарламалардың орнату пакеттері үшін сертификатты шығару
Клиент құрылғыларына бағдарламаларды орнату
Нысанды тексерумен жұмыс
Нысандарды тексеру туралы
Тексерістер журналы бөлімін қарап шығу
Нысанды тексерулерді салыстыру
Нысанды тексерулерді және жойылған нысандар туралы ақпаратты сақтау мерзімін белгілеу
Нысанды тексеруді қарау
Нысанды тексеруді файлда сақтау
Өзгерістерді шегіндіру
Тексерудің сипаттамасын қосу
Нысандарды жою
Нысанды жою
Жойылған нысандар туралы ақпаратты қарау
Нысандарды жойылған нысандар тізімінен жою
Ұялы құрылғыларды басқару
Сценарий: Ұялы құрылғыларды басқаруды орналастыру
iOS MDM құрылғыларын басқаруға арналған топтық саясаттар туралы
Ұялы құрылғыларды басқаруды қосу
Ұялы құрылғыларды басқару параметрлерін өзгерту
Ұялы құрылғыларды басқаруды өшіру
Ұялы құрылғыларға арналған пәрмендермен жұмыс істеу
Ұялы құрылғыларды басқаруға арналған пәрмендер
Firebase Cloud Messaging қолдану

Пәрмендерді жіберу

Пәрмендер журналында пәрмендер күйлерін қарау

Ұялы құрылғыларға арналған сертификаттармен жұмыс істеу

Сертификаттарды орнату шеберін іске қосу

1-қадам. Сертификат түрін таңдау

2-қадам. Құрылғы түрін таңдау

3-қадам. Пайдаланушыны таңдау

4-қадам. Сертификат көзін таңдау

5-қадам. Сертификаттарға тег белгілеу

6-қадам. Сертификатты жариялау параметрлерінің сипаттамасы

7-қадам. Пайдаланушыға хабарлау әдісін таңдау

8-қадам. Сертификат жасау

Сертификаттарды шығару ережелерін конфигурациялау

Жалпыға ортақ кілттер инфрақұрылымымен біріктіру

Kerberos Constrained Delegation қолдауын қосу

iOS ұялы құрылғыларын басқарылатын құрылғылар тізіміне қосу

Android ұялы құрылғыларын басқарылатын құрылғылар тізіміне қосу

iOS MDM құрылғыларын басқару

iOS MDM-профиліне сертификатпен қол қою

Конфигурациялық профильді қосу

Конфигурациялық профильді құрылғыға орнату

Конфигурациялық профильді құрылғыдан жою

Профильге сілтемені жариялау арқылы жаңа құрылғыны қосу

Әкімшінің профильді орнатуы арқылы жаңа құрылғыны қосу

Provisioning профилін қосу

Provisioning профилін құрылғыға орнату

Provisioning профилін құрылғыдан жою

Басқарылатын қолданбаны қосу

Қолданбаны ұялы құрылғыға орнату

Қолданбаны құрылғыдан жою

iOS MDM ұялы құрылғысында роуминг параметрлерін конфигурациялау

iOS MDM құрылғысы туралы ақпаратты қарау

iOS MDM құрылғысын басқарудан өшіру

Құрылғыға пәрмендерді жіберу

Жіберілген пәрмендерді орындау күйін тексеру

KES құрылғыларын басқару

KES құрылғыларына арналған ұялы қолданбалар пакетін жасау

KES құрылғыларының сертификаттары негізінде түпнұсқалықты тексеруді қосу

KES құрылғысы туралы ақпаратты қарау

KES құрылғыларын басқарудан ажырату

Деректерді шифрлау және қорғау

Шифрланған құрылғылар тізімін қарау

Шифрлау оқиғалары тізімін қарау

Шифрлау оқиғаларының тізімін мәтіндік файлға экспорттау

Шифрлау туралы есептерді қалыптастыру және қарау

Басқару серверлері арасында шифрлау кілттерін беру

- Деректер қоймасы
  - Қоймадағы нысандар тізімін мәтіндік файлға экспорттау
  - Орнату пакеттері
  - Қоймадағы файлдардың негізгі күйлері
  - Ережелердің Смарт оқыту режимінде іске қосылуы
    - Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау тізімін қарау
    - Аномалияларды бейімделумен басқару ережесіне ерекшеліктер қосу
      - 1-қадам. Бағдарламаны лицензиялау
      - 2-қадам. Саясатты (саясаттарды) таңдау
      - 3-қадам. Саясатты (саясаттарды) өңдеу
  - Карантин және сақтық көшірмелеу
    - Сақтау орындарындағы файлдарды қашықтан басқаруды қосу
    - Сақтау орнына қойылған файлдың сипаттарын қарап шығу
    - Сақтау орнындағы файлдарды жою
    - Сақтау орнындағы файлдарды қалпына келтіру
    - Сақтау орнындағы файлды дискіге сақтау
    - Карантиндегі файлдарды сканерлеу
  - Белсенді қауіптер
    - Кейін өңделетін файлды дезинфекциялау
    - Кейін өңделетін файлды дискіге сақтау
    - "Белсенді қауіптер" қалтасындағы файлдарды жою
- Kaspersky Security Network (KSN)
  - KSN туралы
  - Kaspersky Security Network бағдарламасына қатынасуды конфигурациялау
  - KSN қосу және өшіру
  - Қабылданған KSN мәлімдемесін қарау
  - KSN прокси-сервері статистикасын қарау
  - Жаңартылған KSN мәлімдемесін қабылдау
  - Kaspersky Security Network көмегімен қосымша қорғау
  - Тарату нүктесі KSN прокси-сервері ретінде жұмыс істейтінін тексеру
- Онлайн-анықтама мен офлайн анықтама арасында ауысу

Оқиғаларды SIEM жүйелеріне экспорттау

- Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау
- Алдын ала шарттар
- Kaspersky Security Center-дегі оқиғалар туралы
- Оқиғаларды экспорттау туралы
- Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау туралы
- SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау
  - Syslog пішімінде экспорттау үшін Kaspersky қолданбасы оқиғаларын жасау
  - Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау
- Syslog пішіміндегі оқиғаларды экспорттау туралы
- CEF және LEEF пішіміндегі оқиғаларды экспорттау туралы
- Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center конфигурациялау

Оқиғаларды тікелей дерекқордан экспорттау
klsql2 утилитасы арқылы SQL сұрауын жасау
klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы
Kaspersky Security Center дерекқорының атауын қарау
Экспорт нәтижелерін қарау
Статистиканы үшінші тарап бағдарламаларына жіберу үшін SNMP пайдалану
SNMP қызметін Kaspersky Security Center-мен пайдалану үшін конфигурациялау
SNMP агенті және нысан идентификаторлары
Нысан идентификаторынан жол есептегіші атауын алу
SNMP үшін нысан идентификаторларының мәндері
Ақаулықтарды жою
Бұлтты ортада жұмыс істеу
Бұлтты ортада жұмыс істеу туралы
Сценарий: Бұлтты ортада орналастыру
Kaspersky Security Center бағдарламасын бұлтты ортада орналастырудың алғышарттары
Бұлтты ортадағы Басқару серверіне қойылатын аппараттық талаптар
Бұлтты ортада лицензиялау нұсқалары
Бұлтты ортада жұмыс істеуге арналған дерекқор параметрлері
Amazon Web Services бұлтты ортасындағы жұмыс
Amazon Web Services бұлтты ортасындағы жұмыс туралы
Amazon EC2 данасы үшін IAM рөлі мен IAM пайдаланушысы есептік жазбаларын жасау
AWS көмегімен Kaspersky Security Center Басқару серверінің жұмыс істеу құқықтарын қамтамасыз ету
Басқару сервері үшін IAM рөлін жасау
Kaspersky Security Center жұмысы үшін IAM пайдаланушысы есептік жазбасын жасау
Amazon EC2 даналарына бағдарламаларды орнату үшін IAM рөлін құру
Amazon RDS-пен жұмыс істеу
Amazon RDS данасын жасау
Amazon RDS данасы үшін параметрлер тобын құру
Параметрлер тобын өзгерту
Amazon RDS дерекқор данасы үшін IAM рөлі құқықтарын өзгерту
Дерекқор үшін Amazon S3 себетін дайындау
Дерекқорды Amazon RDS-ке тасымалдау
Microsoft Azure бұлтты ортасында жұмыс істеу
Microsoft Azure жүйесінде жұмыс істеу туралы
Жазылымды, бағдарлама идентификаторын және құпиясөзді жасау
Azure бағдарламаның идентификаторы үшін рөлді тағайындау
Microsoft Azure жүйесінде Басқару серверін орналастыру және дерекқорды таңдау
Azure SQL-мен жұмыс істеу
Azure сақтау тіркелгісін жасау
Azure SQL дерекқоры мен SQL серверін құру
Дерекқорды Azure SQL-ге тасымалдау
Google Cloud бұлтты ортасында жұмыс істеу
Клиенттің электрондық поштасын, жоба идентификаторын және жеке кілтті жасау
MySQL үшін Google Cloud SQL данасымен жұмыс істеу
Kaspersky Security Center-мен жұмыс істеу үшін бұлтты ортада клиент құрылғыларын дайындау
Бұлтты ортаны конфигурациялау үшін қажетті орнату пакеттерін жасау

- Бұлтты ортаны конфигурациялау
  - Бұлтты ортаны конфигурациялау шебері туралы
  - 1-қадам. Бағдарламаны белсендіру тәсілін таңдау
  - 2-қадам. Бұлтты ортаны таңдау
  - 3-қадам. Бұлтты ортадағы түпнұсқалық растама
  - 4-қадам. Бұлтты ортамен синхрондау және кейінгі әрекеттерді анықтау
  - 5-қадам. Бұлтты ортада Kaspersky Security Network конфигурациялау
  - 6-қадам. Бұлтты ортада электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау
  - 7-қадам. Бұлтты ортада қорғаудың бастапқы конфигурациясын жасау
  - 8-қадам. Орнату барысында операциялық жүйені қайта іске қосу қажет болған кезде әрекетті таңдау (бұлтты орта үшін)
  - 9-қадам. Басқару сервері жаңартуларын алу
- Конфигурацияның сәтті орындалуын тексеру
- Бұлтты құрылғылар тобы
- Бұлттық сегменттерде сауалнама өткізу
  - Бұлттық сегменттерде сауалнама өткізу үшін қосылымдарды қосу
  - Бұлттық сегменттерде сауалнама өткізу үшін қосылымдарды жою
  - Сауалнама кестесін конфигурациялау
- Бағдарламаларды бұлтты ортадағы құрылғыларға орнату
- Бұлтты құрылғылардың сипаттарын қарап шығу
- Бұлтпен синхрондау
- Kaspersky Security Center бағдарламасының Yandex.Cloud ортасындағы жұмыс схемасы

Қолданба

- Кеңейтілген мүмкіндіктер
  - Kaspersky Security Center жұмысын автоматтандыру. klakaut утилитасы
  - Реттелмелі құралдармен жұмыс
  - Желілік агенттің дискісін клондау режимі
  - Операциялық жүйенің бейнесін жасау үшін Желілік агенті орнатылған эталонды құрылғыны дайындау
  - Файл тұтастығын басқару құрамдасынан хабар алу параметрлерін конфигурациялау
  - Басқару серверіне техникалық қызмет көрсету
  - Жалпыға қолжетімді DNS серверлеріне қатынасу
  - Пайдаланушыға хабарлау әдісі терезесі
  - Құрылғы таңдаулары терезесі
  - Жасалатын нысанның атауын анықтау терезесі
- Басқару интерфейсімен жұмыс істеу ерекшеліктері
  - Консоль ағашы
  - Жұмыс аймағындағы деректерді қалай жаңартуға болады
  - Консоль шежіресі бойынша қалай жылжуға болады
  - Жұмыс аймағындағы нысанның сипаттары терезесін қалай ашуға болады
  - Жұмыс аймағындағы нысандар тобын қалай таңдауға болады
  - Жұмыс аймағындағы бағандар жиынтығын қалай өзгертуге болады
- Анықтамалық ақпарат
  - Контекстік мәзір пәрмендері
  - Басқарылатын құрылғылар тізімі Бағандар мәні
  - Құрылғылар, тапсырмалар және саясат күйлері
  - Басқару консоліндегі файлдар күйінің белгішелері

- Деректерді іздеу және экспорттау
  - Құрылғыларды іздеу
  - Құрылғыны іздеу параметрлері
  - Жол айнымалыларында бүркемелерді қолдану
  - Іздеу жолында тұрақты өрнектерді қолдану
  - Диалог терезелеріндегі тізімдерді экспорттау
- Тапсырма параметрлері
  - Тапсырмалардың жалпы параметрлері
  - Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы параметрлері
  - Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасының параметрлері
  - Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері
  - Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы параметрлері
- Глобалды қосалқы желілердің тізімі
  - Глобалды қосалқы желілердің тізіміне ішкі желіні қосу
  - Глобалды қосалқы желілердегі ішкі желінің сипаттарын қарау және өзгерту
- Желілік агентті Windows, Linux және macOS үшін қолдану: салыстыру

Kaspersky Security Center Web Console

- Kaspersky Security Center Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы
- Kaspersky Security Center Web Console бағдарламасы қолданатын порттар
- Kaspersky Security Center Web Console интерфейсі
- Негізгі мәзір бөлімдерін бекіту және бекітуді болдырмау
- Kaspersky Security Center Web Console веб-консолін орнату және бастапқы конфигурациялау
- Орнату
  - Kaspersky Security Center орнату (стандартты орнату)
  - Kaspersky Security Center Web Console орнату
  - Kaspersky істен шығуға төзімді кластерінің түйіндерінде орнатылған Басқару серверіне қосылған Kaspersky Security Center Web Console орнату
  - Kaspersky Security Center Web Console жаңарту
  - Kaspersky Security Center Web Console веб-консолімен жұмыс істеуге арналған сертификаттар
    - Kaspersky Security Center Web Console үшін сертификатты қайта шығару
    - Kaspersky Security Center Web Console үшін сертификатты ауыстыру
    - Сенімді Басқару серверлері үшін сертификаттарды Kaspersky Security Center Web Console веб-консолінде көрсету
    - Сертификатты PFX пішімінен PEM пішіміне түрлендіру
- Kaspersky Security Center Windows жүйесінен деректерді тасымалдау
  - Kaspersky Next Expert View-ге көшу
  - Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы-ке көшіру
  - Kaspersky Security Center Linux бағдарламасына тасымалдау
    - Басқару сервері деректерінің сақтық көшірмесін жасау арқылы Kaspersky Security Center Linux жүйесіне тасымалдау
    - Kaspersky Security Center Linux серверіне тасымалдау шеберімен тасымалдау
      - Kaspersky Security Center Windows жүйесінен топтық нысандарды экспорттау
      - Экспорттық файлын Kaspersky Security Center Linux жүйесіне импорттау
      - Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру
- Kaspersky Security Center Web Console бағдарламасына кіру және одан шығу

Kaspersky Security Center Web Console Есептік деректер және қатынасу диспетчері
Есептік деректер және қатынасу диспетчері құрамдасы туралы
Есептік деректер және қатынасу диспетчерін қосу: сценарий
Kaspersky Security Center Web Console Есептік деректер және қатынасу диспетчерін конфигурациялау
Kaspersky Security Center Web Console веб-консолінде Kaspersky Industrial CyberSecurity for Networks бағдарламаларын тіркеу
Есептік деректер және қатынасу диспетчері үшін авторизацияны күту уақыты және токендердің өміршеңдік уақыты
IAM сертификаттарын жүктеу және тарату
Есептік деректер және қатынасу диспетчерін өшіру
NTLM және Kerberos протоколдарын қолдана отырып, домендік түпнұсқалық растаманы конфигурациялау
Басқару серверін конфигурациялау
Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін конфигурациялау
Басқару серверіне қосылу оқиғасының журналын реттеу
Басқару серверінің интернетке қатынасу параметрлерін конфигурациялау
Оқиғалар қоймасындағы оқиғалар санын конфигурациялау
UEFI деңгейлі қорғанысты құрылғыларды қосу параметрлері
Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу
Қосалқы Басқару серверлері тізімін қарау
Басқару серверлерінің иерархиясын жою
Басқару серверіне техникалық қызмет көрсету
Интерфейсті конфигурациялау
Виртуалды Басқару серверлерін басқару
Виртуалды Басқару серверін жасау
Виртуалды Басқару серверін қосу және өшіру
Виртуалды Басқару сервері әкімшісін тағайындау
Клиент құрылғылары үшін Басқару серверін ауыстыру
Виртуалды Басқару серверін жою
Есептік жазбаны рұқсатсыз өзгертуден қорғауды қосу
Басқару сервері деректерін сақтық көшірмелеу және қалпына келтіру
Деректерді сақтық көшірмелеу тапсырмасын жасау
Басқару серверін басқа құрылғыға тасымалдау
klscmodchk және integrity_checker утилиталарын пайдалану арқылы модульдердің тұтастығын тексеру
Kaspersky Security Center Web Console бастапқы конфигурациялау
Бағдарламаны жылдам іске қосу шебері (Kaspersky Security Center Web Console)
1-қадам. Интернетке қосылу параметрлерін көрсету
2-қадам. Талап етілетін жаңартуларды жүктеп алу
3-қадам. Қорғау үшін активтерді таңдау
4-қадам. Шифрлауды таңдау
5-қадам. Басқарылатын бағдарламалардың плагиндерін орнатуды конфигурациялау
6-қадам. Таңдалған плагиндерді орнату
7-қадам. Дистрибутивтерді жүктеу және орнату пакеттерін жасау
8-қадам. Kaspersky Security Network конфигурациялау
9-қадам. Бағдарламаны белсендіру тәсілін таңдау
10-қадам. Үшінші тарап бағдарламаларының жаңартуларын басқару параметрлерін көрсету
11-қадам. Желі қорғанысының базалық конфигурациясын жасау
12-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

13-қадам. Желіде сауалнама өткізу
14-қадам. Бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау
Автономды құрылғыларды қосу
Сценарий: Автономды құрылғыларды қосылым шлюзі арқылы қосу
Сценарий: демилитаризацияланған аймақтағы Басқару сервері арқылы автономды құрылғыларды қосу
Автономды құрылғыларды қосу туралы
Сыртқы компьютер құрылғыларын басқару серверіне қосу
Автономды пайдаланушыларға арналған қосылым профильдері туралы
Автономды пайдаланушылар үшін қосылым профилін жасау
Желілік агентті басқа Басқару серверіне ауыстырып қосу туралы
Желілік агентті желілік орналасу бойынша ауыстырып қосу ережесін жасау
Қорғанысты орналастыру шебері
1-қадам. Қорғанысты орналастыру шеберін іске қосу
2-қадам. Орнату пакетін таңдау
3-қадам. Кілт файлын немесе белсендіру кодын тарату тәсілін таңдау
4-қадам. Желілік агенттің нұсқасын таңдау
5-қадам. Құрылғыларды таңдау
6-қадам. Қашықтан орнату тапсырмасының параметрлерін орнату
7-қадам. Өшіріп қайта қосуды басқару
8-қадам. Орнатудың алдында үйлесімді емес бағдарламаларды жою
9-қадам. Құрылғыларды басқарылатын құрылғылар қалтасына жылжыту
10-қадам. Құрылғыларға қатынасу үшін есептік жазбаларды таңдау
11-қадам. Орнатуды бастау
Kaspersky бағдарламаларын Kaspersky Security Center Web Console көмегімен орналастыру
Сценарий: Kaspersky бағдарламаларын Kaspersky Security Center Web Console көмегімен орналастыру
Kaspersky бағдарламаларының плагиндерін жүктеу
Kaspersky бағдарламаларына арналған орнату пакеттерін жүктеп алу және жасау
Пайдаланушының орнату пакетінің өлшеміне қойылған шектеулерді өзгерту
Kaspersky бағдарламалары үшін дистрибутивтерді жүктеу
Kaspersky Endpoint Security сәтті орналастырылуын тексеру
Автономды орнату пакетін жасау
Жеке орнату пакеттері тізімін қарау
Пайдаланушы орнату пакетін жасау
Орнату пакеттерін қосалқы Басқару серверлеріне тарату
Қашықтан орнату тапсырмасын пайдаланып бағдарламаларды орнату
Бағдарламаны қашықтан орнату
Active Directory топтық саясаты арқылы бағдарламаны орнату
Қосалқы Басқару серверлеріне бағдарламаларды орнату
Unix басқаруымен жұмыс істейтін құрылғыларда қашықтан орнату параметрлерін көрсету
Kaspersky бағдарламаларын іске қосу және тоқтату
Ұялы құрылғыларды басқару
Үшінші тарап қауіпсіздік бағдарламаларын алмастыру
Желідегі құрылғыларды табу
Сценарий: Желілік құрылғыларды табу
Құрылғыларды табу
Windows желісінің сауалнамасы
IP ауқымдарының сауалнамасы

- IP ауқымын қосу және өзгерту
- Zeroconf сауалнамасы
- Домен контроллері сауалнамасы
- Домен контроллерін аутентификациялау және қосу
- Samba домен контроллерлерін конфигурациялау
- Тағайындалмаған құрылғылар үшін сақтау ережелерін конфигурациялау
- Жабдықты түгендеу
  - Жаңа құрылғылар туралы ақпаратты қосу
  - Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау

Kaspersky бағдарламасы: лицензиялау және белсендіру

- Басқарылатын бағдарламаларды лицензиялау
- Лицензиялық кілтті Басқару серверінің қоймасына қосу
- Басқару серверінің лицензиялық кілтін қосу
- Лицензиялық кілтті клиент құрылғыларына тарату
- Лицензиялық кілтті автоматты түрде тарату
- Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу
- Лицензия кілтін қоймадан өшіру
- Лицензиялық келісімге берілген келісімді кері қайтарып алу
- Kaspersky бағдарламалары лицензиясының әрекет ету мерзімін ұзарту
- Бизнес шешімдерін таңдау үшін Kaspersky Marketplace пайдалану

Желі қорғанысын конфигурациялау

- Сценарий: Желі қорғанысын конфигурациялау
- Құрылғыларға және пайдаланушыларға бағытталған қауіпсіздікті басқару тәсілдемелері
- Саясаттарды конфигурациялау және тарату: құрылғыларға бағытталған тәсілдеме
- Саясаттарды конфигурациялау және тарату: пайдаланушыларға бағытталған тәсілдеме
- Желілік агент саясатының параметрлері
  - Желілік агент саясатының параметрлерін операциялық жүйелер бойынша салыстыру
- Желілік агент үшін ресурстарды аз тұтыну режимін қосу немесе өшіру
- Басқарылатын қолданбалардың қорғаныс параметрлерін конфигурациялау
- Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау
- Бағдарламаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жою
- Тапсырмалар
  - Тапсырмалар туралы
  - Тапсырма аймағы
  - Тапсырманы жасау
  - Тапсырманы қолмен іске қосу
  - Тапсырмалар тізімін қарап шығу
  - Тапсырмалардың жалпы параметрлері
  - Тапсырманы экспорттау
  - Тапсырманы импорттау
  - Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу
    - 1-қадам. Есептік деректерді таңдау
    - 2-қадам. Орындалып жатқан әрекетті таңдау
    - 3-қадам. Нәтижелерді қарап шығу
  - Скрипттерді қашықтан орындау тапсырмасын жасау
    - Скрипттерді қашықтан орындау тапсырмасын пайдаланып құрылғыларға қолданбаларды қашықтан орнату
    - Скрипттерді қашықтан орындау тапсырмасы үшін хабарландыруларды конфигурациялау және бақылау

Скрипттерді қашықтан орындау тапсырмасы үшін мұрағатты дайындау
Манифест-файлы негізінде орнату пакетін жасау
Клиент құрылғыларын басқару
Басқарылатын құрылғының параметрлері
Басқару топтарын жасау
Басқару тобы құрамына құрылғыларды қолмен қосу
Құрылғыларды немесе кластерлерді басқару тобының құрамына қолмен жылжыту
Құрылғыны жылжыту ережелерін жасау
Құрылғыны жылжыту ережелерін көшіру
Құрылғыны жылжыту ережелеріне арналған шарттар
Кластерлер мен серверлердің массивтері туралы
Кластерлердің немесе серверлердің массивтерінің сипаттары
Құрылғы белсенді емес кезде әрекеттерді қарау және конфигурациялау
Құрылғы күйлері туралы
Құрылғылардың күйлерін ауыстыруды конфигурациялау
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу
Windows компьютерлік бөлісу қызметі арқылы құрылғыларға қосылу
Құрылғыны таңдаулары
Құрылғы таңдауларынан құрылғылар тізімін қарау
Құрылғы таңдауларын жасау
Құрылғы таңдауларын конфигурациялау
Құрылғы таңдауларынан құрылғылар тізімін экспорттау
Таңдаудағы басқару топтарынан құрылғыларды жою
Құрылғы тегтері
Құрылғы тегтерін жасау
Құрылғы тегтерін өзгерту
Құрылғы тегтерін жою
Тег тағайындалған құрылғыларды қарап шығу
Құрылғыға тағайындалған тегтерді қарап шығу
Құрылғыға тегтерді қолмен тағайындау
Тағайындалған тегті құрылғыдан жою
Құрылғыларға автоматты түрде тег қою ережелерін қарап шығу
Құрылғыларға автоматты түрде тег қою ережелерін өзгерту
Құрылғыларға автоматты түрде тег қою ережелерін жасау
Құрылғыларға автоматты түрде тег қою ережелерін орындау
Құрылғылардан автоматты түрде тег қою ережелерін жою
klscflag утилитасы арқылы құрылғылар тегтерін басқару
Саясаттар және профильдер
Саясаттар мен саясат профильдері туралы
Бұғаттау (құлып) және бұғатталған параметрлер
Саясат пен саясат профильдерін иелену
Саясаттар иерархиясы
Саясаттар иерархиясындағы саясат профильдері
Басқарылатын құрылғының параметрлері қалай іске асырылады
Саясатты басқару
Саясаттар тізімін қарап шығу
Саясатты жасау

Саясатты өзгерту
Саясаттардың жалпы параметрлері
Саясатты иелену параметрін қосу және өшіру
Саясатты көшіру
Саясатты жылжыту
Саясатты экспорттау
Саясатты импорттау
Саясатты қолдану күйінің диаграммасын қарау
Саясатты жою
Саясат профильдерін басқару
Саясат профильдерін қарау
Саясат профилі басымдығын өзгерту
Саясат профилін жасау
Саясат профилін өзгерту
Саясат профилін көшіру
Саясатын профилін белсендіру ережесін жасау
Саясат профилін жою
Деректерді шифрлау және қорғау
Шифрланған қатты дискілер тізімін қарау
Шифрлау оқиғалары тізімін қарау
Шифрлау туралы есептерді қалыптастыру және қарау
Шифрланған қатты дискіге автономды режимде қатынасу мүмкіндігін ұсыну
Пайдаланушылар және пайдаланушы рөлдері
Пайдаланушы рөлдері туралы
Пайдаланушылардың есептік жазбалары мен сеанстарын қарау
Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау. Рөлге негізделген қатынасуды басқару
Бағдарлама функцияларына қатынасу құқықтары
Алдын ала анықталған пайдаланушы рөлдері
Нысандар жиынтығына қатынасу құқықтарын тағайындау
Пайдаланушыларға немесе қауіпсіздік топтарына құқықтарды тағайындау
Ішкі пайдаланушының есептік жазбасын қосу
Пайдаланушылар тобын жасау
Ішкі пайдаланушының есептік жазбасын өзгерту
Пайдаланушылар тобын өзгерту
Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау
Пайдаланушылардың есептік жазбаларын ішкі қауіпсіздік топқа қосу
Пайдаланушыны құрылғының иесі етіп тағайындау
Барлық пайдаланушы үшін екі қадамдық тексеруді конфигурациялау
Екі қадамдық тексеру туралы
Есептік жазбаңыз үшін екі қадамдық тексеруді қосу (Web Console)
Есептік жазбаңыз үшін екі қадамдық тексеруді қосу (MMC негізінде)
Барлық пайдаланушы үшін міндетті екі қадамдық тексеруді қосу (Web Console)
Барлық пайдаланушы үшін екі қадамдық тексеруді қосу (MMC негізінде)
Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру (Web Console)
Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру (MMC негізінде)
Барлық пайдаланушы үшін міндетті екі қадамдық тексеруді өшіру (Web Console)
Барлық пайдаланушы үшін міндетті екі қадамдық тексеруді өшіру (MMC негізінде)

Есептік жазбаларды екі қадамдық тексеруден алып тастау (Web Console)
Есептік жазбаларды екі қадамдық тексеруден алып тастау (MMC негізінде)
Қауіпсіздік кодын шығарушының атын өңдеу (Web Console)
Қауіпсіздік кодын шығарушының атын өңдеу (MMC негізінде)
Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурациялау (Web Console)
Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурациялау (MMC негізінде)
Жаңа құпия кілтті жасау
Жаңа пайдаланушыларға өздері үшін екі сатылы растауды орнатуға тыйым салу
Желілік агентті орнатқаннан кейін пайдаланушыны Linux құрылғысының иесі ретінде тағайындау
Пайдаланушыларды немесе қауіпсіздік топтарын жою
Пайдаланушы есептік жазбасының құпиясөзін өзгерту
Пайдаланушы рөлін жасау
Пайдаланушы рөлін өзгерту
Пайдаланушы рөлі үшін аймақты өзгерту
Пайдаланушы рөлін жою
Саясат профильдерінің рөлдермен байланысы
Қосалқы Басқару серверлеріне пайдаланушы рөлдерін тарату
Есептік жазбаның құпиясөзін ауыстыру
Жергілікті әкімші құқықтарын кері қайтарып алу
Нысанды тексерумен жұмыс
Нысанның өзгерістерін алдыңғы тексеруге шегіндіру
Тексерудің сипаттамасын қосу
Саясаттың нұсқасын қарау және сақтау
Нысандарды жою
Kaspersky Security Network (KSN)
KSN туралы
KSN бағдарламасына қатынасуды конфигурациялау
KSN қолданысын қосу және өшіру
Қабылданған KSN мәлімдемесін қарау
Жаңартылған KSN мәлімдемесін қабылдау
Тарату нүктесі KSN прокси-сервері ретінде жұмыс істейтінін тексеру
Сценарий: Kaspersky Security Center және басқарылатын қауіпсіздік қолданбаларын жаңарту
Kaspersky дерекқорлары мен бағдарламаларын жаңарту
Сценарий: Kaspersky бағдарламалары мен дерекқорларын үнемі жаңартып тұру
Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту туралы
Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау
Алынған жаңартуларды тексеру
Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау
Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру
Kaspersky Endpoint Security for Windows жаңартуларын автоматты түрде орнату
Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
Басқару серверін жаңарту
Жаңартуларды алудың офлайн-моделін қосу және өшіру
Автономды құрылғыларда Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар
Веб-плагиндерді сақтық көшірмелеу және қалпына келтіру

Тарату нүктелері мен қосылым шлюздерін конфигурациялау
Тарату нүктелерінің типтік конфигурациясы: бір кеңсе
Тарату нүктелерінің типтік конфигурациясы: қашықтағы көптеген шағын кеңселер
Тарату нүктелерін тағайындау туралы
Тарату нүктелерін автоматты түрде тағайындау
Тарату нүктелерін қолмен тағайындау
Басқару тобы үшін тарату нүктелерінің тізімін өзгерту
Мәжбүрлеп синхрондау
Push серверін қосу
Клиент құрылғыларындағы үшінші тарап бағдарламалары бағдарламаларын басқару
Үшінші тарап бағдарламаларының жаңартуларын орнату
Сценарий: Үшінші тарап бағдарламаларын жаңарту
Үшінші тарап бағдарламаларының жаңартуларын орнату
Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау
Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері
Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау
Жаңартуларды орнату үшін ережелер қосу
Windows Update жаңартуларын орнату тапсырмасын жасау
Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау
Қолжетімді жаңартулар тізімін файлға экспорттау
Үшінші тарап бағдарламаларының жаңартуларын мақұлдау және қабылдамау
Windows Update жаңартуларын синхрондау тапсырмасын жасау
Үшінші тарап бағдарламаларын автоматты түрде жаңарту
Үшінші тарап қолданбаларында осалдықтарды түзету
Сценарий: Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету
Бағдарламалық жасақтама осалдықтарын анықтау және түзету туралы
Үшінші тарап қолданбаларында осалдықтарды түзету
Осалдықтарды түзету тапсырмасын жасау
Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау
Жаңартуларды орнату үшін ережелер қосу
Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушы түзетулері
Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау
Таңдалған басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау
Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау
Бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау
Бағдарламалардағы осалдықтарды елемеу
Клиент құрылғыларында бағдарламалардың іске қосылуын басқару
Орындалатын файлдарды басқару үшін Бағдарламаларды басқару компонентін пайдалану
Қолданбаны басқару компонентінің режимдері мен категориялары
Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау
Қолмен қосылған мазмұнмен қолданба санатын жасау
Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау
Таңдалған қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру
Бағдарлама санаттары тізімін қарап шығу
Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу
Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаларды басқару конфигурациялау
Клиент құрылғыларында орнатылған бағдарламалар тізімін алу және қарау

Kaspersky дерекқорынан үшінші тарап бағдарламасы үшін орнату пакетін жасау
Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлерін қарау және өзгерту
Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлері
Бағдарлама тегтері
Бағдарлама тегтерін жасау
Қолданба тегтерін өзгерту
Бағдарламаларға тегтер тағайындау
Бағдарламаларға тағайындалған тегтерді алып тастау
Қолданба тегтерін жою
Бақылау және есеп беру
Сценарий: Бақылау және есеп беру
Бақылау түрлері және есеп беру туралы
Бақылау тақтасы және веб-виджеттер
Бақылау тақтасын қолдану
Ақпараттық тақтаға веб-виджетті қосу
Веб-виджетті ақпараттық тақтадан жою
Веб-виджетті ақпараттық тақтадан жылжыту
Виджеттің өлшемін немесе сыртқы түрін өзгерту
Веб-виджет параметрлерін өзгерту
Тек бақылау тақтасын қарау режимі туралы
Тек бақылау тақтасын қарау режимін конфигурациялау
Басқару және қорғау есептері
Есептерді қолдану
Есеп үлгісін жасау
Есеп үлгісінің сипаттарын қарау және өзгерту
Есепті файлға экспорттау
Есепті жасау және қарау
Есептерді жеткізу тапсырмасын жасау
Есеп үлгілерін жою
Оқиғалар және оқиғаларды таңдау
Kaspersky Security Center-дегі оқиғалар туралы
Оқиға таңдауларын пайдалану
Оқиғалар таңдауын жасау
Оқиғалар таңдауын өзгерту
Оқиғалар таңдауы тізімін қарау
Оқиғалар таңдауын экспорттау
Оқиғалар таңдауын импорттау
Оқиға туралы ақпаратты көру
Оқиғаларды файлға экспорттау
Оқиғадан нысан тарихын қарау
Оқиғаларды жою
Оқиға таңдауларын жою
Оқиғаны сақтау мерзімін конфигурациялау

Kaspersky Security Center құрамдастарының оқиғалары
Оқиға түрі сипаттамасы деректерінің құрылымы
Басқару сервері оқиғалары
Басқару серверінің критикалық оқиғалары
Басқару серверінің функционалдық ақауы оқиғалары
Басқару серверінің ескерту оқиғалары
Басқару серверінің ақпараттық оқиғалары
Желілік агент оқиғалары
Желілік агенттің функционалдық ақауы оқиғалары
Желілік агенттің ескертулері оқиғалары
Желілік агенттің ақпараттық оқиғалары
iOS MDM сервері оқиғалары
iOS MDM серверінің функционалдық ақауы оқиғалары
iOS MDM серверінің ескерту оқиғалары
iOS MDM серверінің ақпараттық оқиғалары
Жиі болатын оқиғаларды бұғаттау
Жиі болатын оқиғаларды бұғаттау туралы
Жиі болатын оқиғаларды бұғаттауды басқару
Жиі болатын оқиғаны бұғаттауды болдырмау
Хабарландырулар және құрылғылар күйлері
Хабарландыруларды қолдану
Экрандағы хабарландыруларды қарау
Құрылғы күйлері туралы
Құрылғылардың күйлерін ауыстыруды конфигурациялау
Хабарландыруларды жеткізу параметрлерін конфигурациялау
Орындалатын файл көмегімен оқиғалар туралы хабарлау
Kaspersky хабарландырулары
Kaspersky хабарландырулары туралы
Kaspersky хабарландыру параметрлерін конфигурациялау
Kaspersky хабарландыруларын өшіру
Табылған қауіптер туралы ақпаратты қарап шығу
Cloud Discovery
Веб-виджетті пайдаланып, Cloud Discovery функциясын қосу
Cloud Discovery веб-виджетін бақылау тақтасына қосу
Бұлттық сервистерді пайдалану туралы ақпаратты қарау
Бұлттық сервистің тәуекел деңгейі
Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттау
Kaspersky Security Center Web Console белсенділік журналы
Kaspersky Security Center бағдарламасын басқа шешімдермен біріктіру
Фондық қосылым орнату
Оқиғаларды SIEM жүйелеріне экспорттау
Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау
Алдын ала шарттар
Kaspersky Security Center-дегі оқиғалар туралы
Оқиғаларды экспорттау туралы
Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау туралы

SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау
SIEM жүйесіне Syslog пішімінде экспорттау үшін оқиғаларды таңдау туралы
Kaspersky бағдарламалары оқиғаларын Syslog пішімінде экспорттау үшін таңдау
Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау
CEF және LEEF пішіміндегі оқиғаларды экспорттау туралы
Оқиғаларды CEF немесе LEEF форматына түрлендіру
Syslog пішіміндегі оқиғаларды экспорттау туралы
Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center конфигурациялау
Оқиғаларды тікелей дерекқордан экспорттау
klsql2 утилитасы арқылы SQL сұрауын жасау
klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы
Kaspersky Security Center дерекқорының атауын қарау
Экспорт нәтижелерін қарау
Kaspersky Security Center Web Console консолімен бұлтты ортада жұмыс істеу
Kaspersky Security Center Web Console веб-консолінде бұлтты ортаны конфигурациялау
1-қадам. Қажетті плагиндер мен орнату пакеттерін тексеру
2-қадам. Қолданбаны лицензиялау
3-қадам. Бұлтты ортаны таңдау және түпнұсқалық растама
4-қадам. Сегмент сауалнамасы, бұлтты ортамен синхрондауды конфигурациялау және кейінгі әрекеттерді анықтау
5-қадам. Саясат пен тапсырмалар жасау үшін бағдарламаны таңдау
6-қадам. Kaspersky Security Center үшін Kaspersky Security Network конфигурациялау
7-қадам. Қорғаудың бастапқы конфигурациясын жасау
Kaspersky Security Center Web Console арқылы желі сегментінде сауалнама өткізу
Бұлттық сегменттерде сауалнама өткізу үшін қосылымдарды қосу
Бұлттық сегменттерде сауалнама өткізу үшін қосылымды жою
Kaspersky Security Center Web Console арқылы сауалнама өткізу кестесін конфигурациялау
Kaspersky Security Center Web Console көмегімен бұлттық сегментте сауалнама өткізу нәтижелерін көру
Kaspersky Security Center Web Console көмегімен бұлтты құрылғылардың сипаттарын көру
Бұлтты сегментпен синхрондау: жылжыту ережесін конфигурациялау
Azure виртуалды машиналарына бағдарламаларды қашықтан орнату
Бұлтты ДҚБЖ көмегімен Басқару сервері деректерін сақтық көшірмелеу тапсырмасын жасау
Клиент құрылғыларын қашықтан диагностикалау
Қашықтан диагностикалау терезесін ашу
Бағдарламалар үшін трассалауды қосу және өшіру
Бағдарламаны трассалау файлын жүктеу
Трассалау файлдарын жою
Бағдарламалар параметрлерін жүктеу
Оқиғалар журналдарын жүктеу
Бағдарламаны іске қосу, тоқтату және қайта іске қосу
Kaspersky Security Center Желілік агент қашықтағы диагностикасын іске қосу және нәтижелерді жүктеп алу
Бағдарламаны клиент құрылғысында іске қосу
Бағдарламадан алынған қоқыс файлын жасау
Linux операциялық жүйесі бар клиенттік құрылғыда қашықтағы диагностиканы іске қосу
Файлдарды Карантинге және Сақтық көшірмелеу жүктеу және одан жою
Файлдарды Карантинге және Сақтық көшірмелеуге жүктеу
Kaspersky Security Center Web Console интерфейсінің тілін өзгерту
API анықтамалық нұсқаулығы

Провайдерлер үшін үздік тәжірибелер
Kaspersky Security Center орналастыруды жоспарлау
Басқару серверіне интернеттен қатынасуды ұсыну
Kaspersky Security Center типтік конфигурациясы
Тарату нүктелері туралы
Басқару серверлерінің иерархиясы
Виртуалды Басқару серверлері
Kaspersky Endpoint Security for Android орнатылған ұялы құрылғыларын басқару
Орналастыру және бастапқы конфигурациялау
Басқару серверін орнату бойынша ұсыныстар
Істен шығуға төзімді кластерде Басқару серверінің қызметтеріне арналған есептік жазбалар жасау
ДҚБЖ таңдау
Басқару серверінің мекенжайын көрсету
Ұйым-клиент желісінде қорғанысты конфигурациялау
Kaspersky Endpoint Security саясатын қолмен конфигурациялау
Кеңейтілген қорғаныс бөлімінде саясатты конфигурациялау
Негізгі қорғаныс бөліміндегі саясатты конфигурациялау
Қосымша параметрлер бөліміндегі саясатты конфигурациялау
Оқиғаларды конфигурациялау бөліміндегі саясатты конфигурациялау
Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау
Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау
Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау
Жаңартуларды орнату және осалдықты түзету топтық тапсырмасын қолмен конфигурациялау
Басқару топтары құрылымын құру және тарату нүктелерін тағайындау
MSP клиентінің типтік конфигурациясы: бір кеңсе
MSP клиентінің типтік конфигурациясы: көптеген шағын оқшауланған кеңселер
Саясаттар иерархиясы, саясат профильдерін қолдану
Саясаттар иерархиясы
Саясат профильдері
Тапсырмалар
Құрылғыны жылжыту ережелері
Бағдарламалық жасақтаманы санаттау
Бірнеше қатысушысы бар бағдарламалар туралы
Басқару сервері параметрлерін сақтық көшірмелеу және қалпына келтіру
Басқару сервері бар құрылғы істен шықты
Басқару серверінің параметрлері немесе дерекқор зақымдалған
Желілік агент пен қауіпсіздік бағдарламасын орналастыру
Бастапқы орналастыру
Инсталляторлар параметрлерін конфигурациялау
Орнату пакеттері
MSI сипаттары және түрлендіру файлдары
Қолданбаларды қашықтан орнатудың үшінші тарап құралдары арқылы орналастыру
Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмалары туралы жалпы мәліметтер
Microsoft Windows топтық саясаттары тетігінің көмегімен орналастыру
Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру
Kaspersky Security Center қалыптастырған автономды пакеттерді іске қосу
Қолданбаларды қолмен басқару мүмкіндіктері

Желілік агенті орнатылған құрылғыларға бағдарламаларды қашықтан орнату
Қашықтан орнату тапсырмасында құрылғыларды қайта жүктеуді басқару
Антивирустық қолданбаның орнату пакетіндегі дерекқорларды жаңартудың орындылығы
Үшінші тараптардың үйлесімсіз қауіпсіздік бағдарламаларын жою
Пәрмен желісі арқылы құпиясөзбен қорғалған Желілік агентті жою
Ерікті орындалатын файлдардың басқарылатын құрылғыларында іске қосу үшін Kaspersky Security Center қолданбаларын қашықтан орнату құралдарын қолдану
Орналастыру мониторингі
Инсталляторлар параметрлерін конфигурациялау
Жалпы ақпарат
Тыныш режимде орнату (жауаптар файлымен)
Желілік агентті тыныш режимде орнату (жауаптар файлы жоқ)
setup.exe арқылы орнату параметрлерін ішінара конфигурациялау
Басқару серверін орнату параметрлері
Желілік агентті орнату параметрлері
Виртуалды инфрақұрылым
Виртуалды машиналарға түсетін жүктемені азайту бойынша ұсынымдар
Динамикалық виртуалды машиналарды қолдау
Виртуалды машиналарды көшіруді қолдау
Желілік агенті бар құрылғылар үшін файлдық жүйені шегіндіруді қолдау
Автономды пайдаланушыларға арналған қосылым профильдері туралы
Ұялы құрылғыларды қолдауды орналастыру
KES құрылғыларын Басқару серверіне қосу
Құрылғыларды Басқару серверіне тікелей қосу
Kerberos (KCD) мәжбүрлеп табыстау арқылы KES құрылғыларын Серверге қосу схемасы
Firebase Cloud Messaging қолдану
Жалпыға ортақ кілттер инфрақұрылымымен біріктіру
Kaspersky Security Center Web Server
Басқа да күнделікті тапсырмалар
Басқару консолінде түс индикаторлары мен тіркелген оқиғаларды мониторингтеу
Басқарылатын құрылғыларға қашықтан қатынасу
Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін "Басқару серверімен байланысты үзбеу" параметрін қолдану
Құрылғыны Басқару серверіне қосу уақытын тексеру туралы
Мәжбүрлеп синхрондау туралы
Туннельдеу туралы
Өлшеу нұсқаулығы
Осы нұсқаулық туралы
Kaspersky Security Center шектеулері туралы ақпарат
Басқару серверлері үшін есептеулер
Басқару сервері үшін аппараттық ресурстарды есептеу
ДҚБЖ және Басқару серверіне арналған аппараттық талаптар
Дерекқорда орынды есептеу
Дискідегі орынды есептеу (Осалдықтар мен патчтарды басқаруды пайдалануды ескере отырып және есепке алмай)
Басқару серверлерінің саны мен конфигурациясын есептеу
Динамикалық виртуалды машиналарды Kaspersky Security Center бағдарламасына қосу бойынша ұсыныстар

Тарату нүктелері мен қосылым шлюздеріне арналған есептеулер
Тарату нүктесі үшін талаптар
Тарату нүктелерінің саны мен конфигурациясын есептеу
Қосылым шлюздерінің санын есептеу
Тапсырмалар мен саясаттар үшін оқиғалар туралы ақпаратты сақтау
Кейбір тапсырмалардың ерекшеліктері мен оңтайлы параметрлері
Құрылғыны табу жиілігі
Басқару сервері деректерінің резервтік қоймасы және Басқару серверіне қызмет көрсету тапсырмалары
Kaspersky Endpoint Security жаңарту топтық тапсырмалары
Түгендеу тапсырмасы
Басқару сервері мен қорғалатын құрылғылар арасында желіге түсетін жүктеме туралы ақпарат
Әртүрлі сценарийлерді орындау кезіндегі трафик шығыны
Трафиктің тәулік ішіндегі орташа шығыны
Техникалық қолдау қызметіне жүгіну
Техникалық қолдау алу жолдары
Kaspersky CompanyAccount арқылы техникалық қолдау
Басқару серверінің қоқыс файлдарын алу
Бағдарлама мәліметтері көздері
Глоссарий
Amazon EC2 даналары
Amazon есептеуіш машинасының кескіні (AMI)
AWS Application Program Interface (AWS API)
AWS IAM қатынас кілті
AWS басқару консолі
Cloud Discovery
FileTransferBridge
HTTPS
IAM пайдаланушысы
IAM рөлі
Identity and Access Management (IAM)
iOS MDM құрылғы
iOS MDM профилі
iOS MDM сервері
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center Web Server
Kaspersky Security Center әкімшісі
Kaspersky Security Center қолданбасын жаңарту
Kaspersky Security Center операторы
Kaspersky Security Network (KSN)
Kaspersky жаңарту серверлері
KES құрылғылары
MITM шабуылы
Network Location Awareness (NLA)
Provisioning профилі
SSL

UEFI деңгейінде қорғанысы бар құрылғы

Windows Server Update Services (WSUS)

Антивирустық дерекқорлар

Антивирустық қорғаныс провайдері

Арнайы құрылғыға арналған тапсырма

Әкімшілік құқықтар

Әкімшінің жұмыс станциясы

Бағдарлама параметрлері

Бағдарламаларды орталықтандырылған басқару

Бағдарламаны тікелей басқару

Басқару консолі

Басқару плагині

Басқару сервері

Басқару сервері деректерін сақтық көшірмелеу

Басқару сервері сертификаты

Басқару серверінің деректерін қалпына келтіру

Басқару серверінің клиенті (Клиент құрылғысы)

Басқару тобы

Басқарылатын құрылғылар

Белсенді кілт

Бұлтты орта

Виртуалды Басқару сервері

Вирустық белсенділік шегі

Вирустық шабуыл

Демилитаризацияланған аймақ (DMZ)

Жалпы сертификат

Жаңарту

Желілік агент

Желінің антивирустық қорғанысы

Желінің қорғаныс күйі

Жеңіл N агенті (LWNGT)

Жергілікті тапсырма

Жергілікті түрде орнату

Ішкі пайдаланушылар

Кеңінен тарататын домен

Кілт файлы

Клиент әкімшісі

Конфигурациялық профиль

Күшпен орнату

Қалпына келтіру

Қашықтан орнату

Қолданбалар дүкені

Қолжетімді жаңарту

Қолмен орнату

Қорғаныс күйі

Қорғанысты күшейту нұсқаулығы

Қосылым шлюзі

Қосымша (немесе резервтегі) лицензиялық кілт
Құрылғының иесі
Лицензия мерзімі
Лицензиялы бағдарламалар тобы
Оқиғалар қоймасы
Оқиғаның маңыздылық деңгейі
Орнату пакеті
Осалдық
Патчтың маңыздылық деңгейі
Провайдер әкімшісі
Сақтық көшірме қоймасы
Саясат
Тапсырма
Тапсырма параметрлері
Тарату нүктесі
Топтық тапсырма
Түпнұсқалық растама агенті
Үйдегі Басқару сервері
Үйлесімсіз бағдарлама
Ұялы құрылғылардың сервері
Үшінші тарап коды туралы ақпарат
Тауар белгілері туралы хабарландырулар
Шектеулер тізімі

Kaspersky Security Center 15.1 бағдарламасына анықтама

	**Не жаңалық** Бағдарламаның осы нұсқасында не жаңалық бар екенін біліңіз.		**Желі қорғанысын конфигурациялау** Ұйымның қауіпсіздігін басқару.
	**Аппараттық және бағдарламалық талаптар** Қолдау көрсетілетін операциялық жүйелер мен бағдарлама нұсқаларын тексеріңіз.		**Kaspersky бағдарламалары. Дерекқорлар мен бағдарламалық модульдерді жаңарту** Қорғаныс жүйесінің сенімділігін қолдау
	**Орналастыру және бастапқы конфигурациялау** Ресурстарды жоспарлау: Басқару серверін орнату, клиент құрылғыларында Желілік агент пен қауіпсіздік бағдарламаларын орнату, құрылғыларды басқару топтарына біріктіру.		**Бақылау және есеп беру** Желіңіздің инфрақұрылымы, қорғаныс күйі және статистика туралы деректерді қарау. Cloud Discovery көмегімен бұлтты қызметтерге кіруді басқару.
	**Желідегі құрылғыларды табу** Ұйымыңыздың желісінде бұрыннан бар және жаңа құрылғыларды табу.		**Үшінші тарап қауіпсіздік бағдарламаларын алмастыру** Үйлесімсіз бағдарламаларды жою әдістері туралы біліңіз.
	**Kaspersky бағдарламалары. Орталықтандырылған орналастыру** Kaspersky қолданбаларын орналастыру.		**Тарату нүктелері мен қосылым шлюздерін конфигурациялау** Тарату нүктелерін конфигурациялау.
	**Kaspersky Security Center алдыңғы нұсқасын жаңарту** Kaspersky Security Center 15.1 бағдарламасын алдыңғы нұсқадан жаңарту.		**Провайдерлерге арналған үздік тәжірибелер (тек онлайн-анықтама ғана)** Бағдарламаны орналастыру, конфигурациялау және пайдалану бойынша ұсыныстар, сондай-ақ бағдарлама жұмыс істеген кезде туындайтын типтік мәселелерді шешу тәсілдерімен танысыңыз.
	**Kaspersky бағдарламалары. Лицензиялау және белсендіру** Kaspersky бағдарламаларын бірнеше қадаммен белсендіру.		**Өлшеу нұсқаулығы (тек онлайн-анықтама)** Әртүрлі шарттарда оңтайлы өнімділік үшін, желідегі құрылғылардың санын, желі топологиясын және өзіңізге қажетті Kaspersky Security Center функциялар жиынтығын ескеруіңіз керек.
	**Оқиғаларды SIEM жүйелеріне экспорттау** Талдау үшін оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялаңыз.		**Осалдықтар мен патчтарды басқару** Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету.
	**Бұлтты ортада жұмыс істеу** Kaspersky Security Center бұлтты ортада орналастыру: Amazon Web Services™, Microsoft Azure™, Google™ Google Cloud платформасы.		**Жиі қойылатын сұрақтар (тек ағылшын тілінде)** Кеңінен таралған мәселелерді шешуге арналған нұсқауларды табыңыз.
	**Kaspersky Endpoint Security for Business бағдарламасымен жұмысты бастау туралы қысқаша нұсқаулық** Kaspersky Endpoint Security for Business бағдарламасымен жұмысты бастаңыз: бұл шешімді орнатыңыз және конфигурациялаңыз. Сондай-ақ, желі қауіпсіздігін басқарудың ең қолайлы тәсілін таңдау үшін Kaspersky Security Center функцияларын салыстыруды көруге болады.		

Не жаңалық

Kaspersky Security Center 15.1 2-жаңартуы

Kaspersky Security Center 15.1 2-жаңартуы пайдаланушылар мен сынау тобы хабарлаған мәселелерді шешуге бағытталған:

- TXT файлын импорттау арқылы көрсетілген Linux негізіндегі басқарылатын құрылғылар ауқымы үшін тапсырмалар енді дұрыс орындалады.
- Енді Kaspersky қолданбасы виртуалдық басқару серверінде жасалған қашықтан орнату тапсырмасымен орнатылған кезде, орнату пакеттері операциялық жүйе құралдары арқылы басқарылатын құрылғыларға тек сол виртуалдық басқару сервері басқаратын тарату нүктесі арқылы тасымалданады.
- Қосалқы Басқару сервері қосалқы сервер сертификатын айналдырғаннан кейін негізгі басқару серверіне қайта қосыла алмайтын мәселе шешілді.
- TLS қосылымдарына әсер ететін мәселелер шешілді.
- Пайдаланушы кірген кезде бірнеше "Жарамсыз теру" қатесін тудырған мәселе шешілді.
- Kaspersky Security Center енді оқиға туралы хабарландыруларды электрондық хат арқылы дұрыс жібереді.
- *Kaspersky Security Center 14.2 нұсқасынан 15.1 нұсқасына жаңарту* кезінде сақтық көшірмеге Жаңартулар қалтасын қосу мәселесі шешілді.
- Kaspersky қолданбасы лицензиясының жарамдылық мерзімі енді Kaspersky Security Center Web Console-де дұрыс көрсетіледі.
- **Ұялы құрылғының орналасуын алу** және **Құрылғы орнының журналын алу** пәрмендері енді дұрыс жұмыс істейді.
- Мобильдік сертификаттары бар орнату пакеттерін жүктеп алған соң 1 сағаттан кейін немесе пайдаланылмаған күйде қалған соң 24 сағаттан кейін автоматты түрде жойылмайтын мәселе түзетілді.
- Арнайы тэг арқылы белсендірілген саясат профиль енді сипаттамаларында осы тэг бар құрылғыларға дұрыс қолданылады.
- Оқиға журналында PostgreSQL дерекқор қатесі туралы хабарлардың пайда болуына әкелген мәселе түзетілді.
- Есептік жазбаны екі қадамдық тексеруден шығару енді дұрыс жұмыс істейді.
- Есептік деректер және қатынасу диспетчері қосылған домен аутентификациясын пайдаланған кезде Kaspersky Security Center Web Console жүйесінен шығу дұрыс жұмыс істемейтін мәселе түзетілді.
- Енді басқару веб-плагинін жаңарту кезінде қажетті плагин нұсқасы бар сілтемені басу жүктеп алу әрекетін бастайды.

- Есептерге қатысты түзетілген мәселелер:
  - Қауіп-қатер туралы есептер мен жаңартулар үшін жеткізу тапсырмасын жасағанда және тапсырма кестесін **Ай сайын** мәніне орнатқанда, есептер деректермен дұрыс толтырылады.
  - *Қолданба компоненттерінің күйі туралы есеп* үлгісінде сүзгілер компонент атауы бойынша дұрыс қолданылады.
  - Енді *қорғанысты орналастыру туралы есепті* тек Kaspersky қолданбалары орнатылмаған құрылғыларды көрсететіндей сүзгілеуге болады. Бұл қолданбалар орнатылған құрылғылардың санын визуализациялауға көмектеседі.
- **Cloud Discovery** виджеті Жалпы мүмкіндіктер: негізгі функциялар **аймағында** Орындау **құқығы** бар-жоғына қарамастан дұрыс көрсетіледі.
- Сақталған процедуралар мен дерекқор операцияларының өнімділігі жақсартылды.
- Жоқ пайдаланушылармен байланысты мерзімі өткен сертификаттар барлық пайдаланушылар үшін жаңарту процесінің тоқтауына әкелетін мәселе түзетілді.
- Сертификаттарды дұрыс өңдеуге әсер ететін мәселелер шешілді.
- Kaspersky Security Center 14.2 нұсқасынан 15.1 нұсқасына жаңартқаннан кейін, басқару консоліндегі қосалқы виртуалдық басқару серверінен оқшау орнату пакетін жүктеп алу әрекеті енді дұрыс жұмыс істейді.
- Kaspersky Security Center Web Console-де Kaspersky қолданбасының саясатында Kaspersky Security Network (KSN) пайдалануды қосқанда, KSN мәлімдемесін қабылдау келесі қолданбалар үшін қолжетімді болмады: Kaspersky Endpoint Security for Linux 12.2 немесе одан бұрынғы нұсқасы, Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 немесе одан бұрынғы нұсқасы, Kaspersky Security for Virtualization Light Agent 6.0 және 6.1 нұсқасы, Kaspersky Embedded Systems Security for Linux 3.3 нұсқасы және Kaspersky Security for Windows Server 11.0.1.897 нұсқасы.
- Саясат профилі Active Directory домен тобына енгізілген Linux негізіндегі құрылғыларға қолданылмаған мәселе түзетілді.
- Екінші деңгейлі бірнеше қосалқы басқару серверінен негізгі басқару серверіне қосылу әрекеттері кезінде орын алған мәселе түзетілді.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Cloud Discovery. Қолданбасының жаңа функционалдығы Windows операциялық жүйесімен жұмыс істейтін басқарылатын құрылғыларда бұлттық қызметтерді пайдалануды бақылауға және қажетсіз бұлттық қызметтерге кіруді бұғаттауға мүмкіндік береді. Бұл мүмкіндік тек Kaspersky Security Center Web Console веб-консолінде қол жетімді.
- Домен контроллеріне сауалнама жүргізу енді Linux операциялық жүйесі бар тарату нүктесі арқылы Samba домен контроллерлеріне сауалнама жүргізуге мүмкіндік береді. Үлкен домендерге сауалнама жүргізуге қолдау көрсетуге арналған қосымша түзетпелер.
- Linux операциялық жүйесімен жұмыс істейтін басқарылатын құрылғыларды қашықтан кеңейтілген диагностикалау.

- MacOS құрылғыларының жабдықтарын кеңейтілген түгендемесі. macOS құрылғысындағы Желілік агент құрылғының MAC мекенжайы мен сериялық нөмірін Басқару серверіне жібереді.

- Енді SIEM жүйесінің қосылымын тексере аласыз.

- Ішкі пайдаланушы үшін құпиясөздің максималды ұзындығы 256 таңбаға дейін ұлғайтылды.

- Енді деректерді Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне тасымалдаған кезде деректердің сақтық көшірмесінен басқару серверінің сертификаты мен жеке кілтін қалпына келтіру арқылы Kaspersky Security Center Linux басқаратын құрылғыларды ауыстыруға болады.

- Құпиясөзбен қорғалған Желілік агентті жою үшін Cleaner немесе klmover утилитасын іске қосқанда, жоюға арналған құпиясөзді енгізу сұралады.

- Kaspersky Security for Windows Server жүйесінен Kaspersky Endpoint Security for Windows жүйесіне жаңарту үшін бұдан былай мақсатты құрылғыны қайта жүктеу талап етілмейді.

- Пайдаланушы Желілік агентті Linux жүйесімен жұмыс істейтін клиенттік құрылғыға орнату кезінде немесе орнатқаннан кейін құрылғы иесі ретінде тағайындалуы мүмкін.

- Басқарылатын құрылғыларға бағдарламалық жасақтаманы пайдаланушылық скрипттерді пайдаланып орнатқанда, енді қашықтан орнату есебін алуға болады.

- Басқарылатын құрылғыда бірнеше пайдаланушылық скриптті орындаған кезде, олардың орындалу ретін анықтау үшін әрбір сценарийге басымдық беруге болады. Скрипттер ең жоғары басымдықты скрипттен ең төменгі басымдықты скриптке дейін орындалады.

- Кеңейтілген саясаттар аудиті. Енді сіз саясаттың тексерісін көре аласыз және саясаттың тексерісін файлға сақтай аласыз. Қазіргі уақытта бұл мүмкіндіктер тек Басқару сервері және Желілік агент саясаттары үшін қолжетімді.

- Пайдаланушы тәжірибесін жақсарту, соның ішінде:

  - **Бекітілген** бөлімнен жылдам қол жеткізу үшін Kaspersky Security Center Web Console бөлімдерін бекіту арқылы негізгі мәзірді жекелендіру.

  - Кестелермен жұмыс оңтайландырылды. Әрбір кесте үшін әдепкі көрініс енді ең жиі қолданылатын бағандарды қамтиды. Сондай-ақ, енді ағымдағы беттегі немесе бүкіл кестедегі барлық элементтерді таңдап, элементтерді бүкіл кесте бойынша сұрыптауға болады.

  - Есептерді тарату конфигурациясы жақсартылды. Енді есепті тарату үшін 20 электрондық пошта мекенжайына дейін көрсетуге және есепті тарату кестесін белгілеуге болады.

- Linux операциялық жүйесі бар басқарылатын құрылғыларда жергілікті есептік жазбалар әкімшісі құқықтарын қайтарып алуға болады. Бұл пайдаланушы есептік жазбаларын бақылаудың қосымша деңгейін береді. Мысалы, бір реттік тапсырманы орындағаннан кейін жергілікті әкімші құқықтарын жоя аласыз.

- Linux операциялық жүйесі бар басқарылатын құрылғыларда жергілікті есептік жазба құпиясөзін өзгертуге болады (мысалы, пайдаланушы жергілікті есептік жазба құпиясөзін ұмытып қалғанда немесе құпиясөзді кесте бойынша өзгерту үшін).

- **Пайдаланушы сертификаттарын басқару** ішкі бөлімінде қай түбірлік сертификаттарды орнату керектігін көрсетуге болады. Бұл сертификаттарды, мысалы, веб-сайттардың немесе веб-серверлердің түпнұсқалығын тексеру үшін пайдалануға болады.

- Желілік шабуылдар туралы есеп енді шабуылдаушы құрылғының MAC мекенжайы мен портын қамтиды.

- Ішкі пайдаланушының Kaspersky Security Center Web Console веб-консоліне келесі жолы кірген кезде құпиясөзді өзгертуді талап ететін жаңа параметр.
- Оқиғаларды SIEM жүйесіне CEF немесе LEEF пішімінде экспорттау кезінде коммерциялық лицензия енді тексерілмейді.
- Деректерді бір Kaspersky қолданбасынан екіншісіне тасымалдап жатсаңыз және ағымдағы қолданба құпиясөзбен қорғалған болса, енді жою құпиясөзін қашықтан орнату тапсырмасында тікелей көрсетуге болады.
- Exchange ActiveSync протоколына енді қолдау көрсетілмейді.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Қорғаныс күшейту нұсқаулығы шығарылды. Kaspersky Security Center және желілік инфрақұрылымыңызды конфигурациялау кезінде нұсқаулықты мұқият оқып шығуды және қауіпсіздік ұсыныстарын орындауды қатаң ұсынамыз.

  Сондай-ақ, Kaspersky Security Center соңғы жаңартуын орнатыңыз. Бұл жаңарту, пайдаланушы есептік жазбаларын екі қадамдық тексеру және басқа жақсартулар сияқты инфрақұрылымды қорғау функцияларын қамтиды.
- Kaspersky серверлеріне қатынасу енді автоматты түрде тексеріледі. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS жүйесін пайдаланады.
- Виртуалды Басқару сервері пайдаланушысының құқықтары басты Басқару сервері пайдаланушыларының құқықтарына қарамастан конфигурацияланады. Сондай-ақ, сіз басты Сервер пайдаланушыларына виртуалды Серверді басқару құқығын да бере аласыз.
- Kaspersky Security Center енді келесі ДҚБЖ-мен жұмысты қолдайды:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (барлық басылым).
  - Postgres Pro 14.x (барлық басылым).
  - MariaDB 10.1, 10.4, 10.5.
- Сіз Kaspersky Security Center Web Console веб-консолін саясаттар мен тапсырмаларды файлға экспорттау, содан соң саясаттар мен тапсырмаларды Kaspersky Security Center Windows немесе Kaspersky Security Center Linux операциялық жүйелеріне импорттау үшін қолдана аласыз.
- **Прокси-серверді пайдаланбау** параметрі келесі тапсырмалардан жойылған:
  - *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*
  - *Жаңартуларды тарату орындарының қоймаларына жүктеп алу*

- Бұлтты ортадағы клиент құрылғыларын қорғау үшін Kaspersky Security for Windows Server орнына Kaspersky Endpoint Security for Windows орналастыруға болады. Бұл функция Kaspersky Endpoint Security 12.0 for Windows жаңа нұсқасы шыққаннан кейін қолжетімді болады.

- Шифрлау кілттерімен жұмыс істеу енді **Жалпы функционал**: **Шифрлау кілтін басқару** функционалдық аймағындағы қатынасу құқықтарымен шектеледі. Kaspersky Security Center пайдаланушылары енді **Оқу** құқығы болса, шифрлау кілттерін экспорттай алады және **Жазу** құқығы болса, шифрлау кілттерін импорттай алады.

Kaspersky Security Center 14

Kaspersky Security Center 14 бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Оқшауланған желіде үшінші тарап бағдарламаларының (Microsoft бағдарламаларынан басқа) осалдықтарын жауып, жаңартуларын орната аласыз. Мұндай желілерге, интернетке қатынаса алмайтын Басқару серверлері мен басқарылатын құрылғылар жатады. Мұндай желідегі осалдықтарды жабу үшін интернетке қатынасы бар Басқару серверін пайдалану арқылы қажетті жаңартуларды жүктеп, патчтарды оқшауланған Басқару серверлеріне жіберу керек.

- macOS құрылғылары үшін автономды пайдаланушыларға арналған қосылым профильдері қосылған. Қосылым профильдерінің көмегімен сіз macOS құрылғыларындағы Желілік агенттерді құрылғының орналасқан жеріне байланысты бірдей немесе әртүрлі Басқару серверлеріне қосу ережелерін конфигурациялай аласыз.

- Енді Желілік агентті Microsoft Windows 10 IoT Enterprise орнатылған құрылғыларға орнатуға болады.

- **Қауіп-қатер туралы есеп** есебінде енді қауіптер тізімін Cloud Sandbox анықтаған қауіптерді ғана көру үшін сүзгілеуге болады.

- Kaspersky Security Center енді Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 бағдарламасын басқарылатын бағдарлама ретінде қолдайды.

Kaspersky Security Center Web Console бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Желіні басқармайтын, бірақ Kaspersky Security Center-де желі қорғанысы статистикасын көргісі келетін қызметкерлер үшін Тек бақылау тақтасын қарау режимін конфигурациялауға болады (мысалы, бұл топ-менеджер болуы мүмкін). Пайдаланушыда осы режим қосулы болғанда, алдын ала анықталған веб-виджеттер жиынтығы бар бақылау тақтасы ғана көрсетіледі. Осылайша, пайдаланушы веб-виджеттерде көрсетілген статистиканы, мысалы, барлық басқарылатын құрылғылардың қорғаныс күйін, жақында табылған қауіптер санын немесе желідегі ең көп таралған қауіптер тізімін көре алады.

- Kaspersky Security Center Web Console веб-консолі Kaspersky Security for iOS қолданбасын қауіпсіздік бағдарламасы ретінде қолдайды.

- Тапсырма сипаттарында, тапсырманы ішкі топтарға және қосалқы Басқару серверлеріне (соның ішінде виртуалды) қолданғыңыз келеді ме екенін көрсете аласыз.

- Kaspersky Security Center енді Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 бағдарламасын басқарылатын бағдарлама ретінде қолдайды.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Енді сіз келесі жаңа операциялық жүйелер үшін Басқару серверін, Басқару консолін, Kaspersky Security Center 13.2 Web Console және Желілік агентті орната аласыз (бағдарламалық жасақтамаға қойылатын талаптарды қараңыз):
  - Microsoft Windows 11.
  - Microsoft Windows 10 21H2 (October 2021 Update).
  - Microsoft Windows Server 2022.
- MySQL 8.0 дерекқорын қолдана аласыз.
- Kaspersky Security Center бағдарламасының жоғары қолжетімділігін қамтамасыз ету үшін Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінде орналастыра аласыз.
- Kaspersky Security Center енді IPv6 мекенжайларымен де, IPv4 мекенжайларымен де жұмыс істейді. Басқару сервері IPv6 мекенжайлары бар құрылғылар қамтылған желілерді сұрастыруы мүмкін.

Kaspersky Security Center 13.2 Web Console бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- Енді сіз Kaspersky Security Center 13.2 Web Console көмегімен Android операциялық жүйесі бар ұялы құрылғыларды басқара аласыз.
- Kaspersky Marketplace, мәзірдің жаңа бөлімі түрінде қолжетімді: сіз Kaspersky Security Center 13.2 Web Console арқылы Kaspersky бағдарламаларын іздей аласыз.
- Kaspersky Security Center енді келесі Kaspersky бағдарламаларын қолдайды:
  - Kaspersky Endpoint Detection and Response Optimum 2.0.
  - Kaspersky Sandbox 2.0.
  - Kaspersky Industrial CyberSecurity for Networks 3.1.

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 бағдарламасында бірнеше жаңа функциялар мен жақсартулар іске асырылған:

- SIEM жүйелерімен біріктіру жақсартылған. Енді сіз оқиғаларды шифрланған арна (TLS) арқылы SIEM жүйелеріне экспорттай аласыз. Функция Kaspersky Security Center Web Console үшін және Microsoft Management Console (MMC) консолі негізіндегі Басқару консольдері үшін қолжетімді.
- Басқару серверіне арналған түзетулерді, ең соңғы нұсқаларға дейінгі болашақ жаңартулар үшін қолдануға болатын дистрибутив түрінде ала аласыз.

- Kaspersky Security Center 13.1 Web Console веб-консоліне Kaspersky Endpoint Detection and Response Optimum үшін **Анықтау** бөлімі қосылды. Сондай-ақ, Kaspersky Endpoint Detection and Response Optimum анықтаған қауіптермен жұмыс істеу үшін бірнеше веб-виджет те қосылған.

- Kaspersky Security Center 13.1 Web Console веб-консолінде Kaspersky бағдарламаларына арналған лицензиялардың әрекет ету мерзімінің өтіп кеткені туралы хабарландыруларды ала аласыз.

- Kaspersky Security Center 13.1 Web Console жауап беру уақыты қысқартылды.

Kaspersky Security Center 13

Kaspersky Security Center 13 Web Console бағдарламасында келесі функциялары іске асырылды:

- Екі қадамдық тексеру енгізілген. Kaspersky Security Center 13 Web Console веб-консоліне рұқсатсыз қатынасу қатерін төмендету үшін екі қадамдық тексеруді қоса аласыз.

- NTLM және Kerberos протоколдарын (бірыңғай кіру) қолдану арқылы домендік түпнұсқалық растама енгізілген. Бірыңғай кіру функциясы, Windows пайдаланушысына корпоративтік желіде құпиясөзді қайта енгізбей-ақ, Kaspersky Security Center 13 Web Console веб-консолінде қауіпсіз түпнұсқалық растаманы қосуға мүмкіндік береді.

- Енді сіз Kaspersky Managed Detection and Response бағдарламасымен жұмыс істеуге арналған плагинді конфигурациялай аласыз. Сіз осылай біріктіруді инциденттерді қарап шығу және жұмыс станцияларын басқару үшін қолдана аласыз.

- Енді сіз Kaspersky Security Center 13 Web Console параметрлерін Басқару серверін орнату шеберінде көрсете аласыз.

- Жаңартулар мен патчтардың жаңа шығарылымы туралы хабарландырулар көрсетіледі. Сіз жаңартуды бірден немесе кейінірек кез келген уақыта орната аласыз. Енді сіз Басқару серверіне арналған патчтарды Kaspersky Security Center 13 Web Console көмегімен орната аласыз.

- Кестелермен жұмыс істеу кезінде, енді бағандардың реті мен енін көрсетуге, деректерді сұрыптауға және беттің өлшемін көрсетуге болады.

- Кез келген есепті оның атын басу арқылы аша аласыз.

- Kaspersky Security Center 13 Web Console бағдарламасының интерфейсі және онлайн-анықтама енді кәріс тілінде де қолжетімді.

- Kaspersky хабарландыруларының жаңа бөлімі **Бақылау және есеп беру** бөлімінде қолжетімді. Бұл бөлімде Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларда орнатылған басқарылатын бағдарламалар туралы ақпарат көрсетілген. Kaspersky Security Center бағдарламасы бөлімдегі ақпаратты жаңартады, ескірген хабарландыруларды жояды және жаңа ақпаратты қосады. Kaspersky хабарландыруларын өшіруіңізге болады.

- Пайдаланушы есептік жазбалары параметрлерін өзгерткеннен кейін, қосымша түпнұсқалық растама іске асырылған. Сіз пайдаланушының есептік жазбасын рұқсатсыз өзгертуден қорғауды қоса аласыз. Бұл параметр қосулы болса, пайдаланушының есептік жазбасының параметрлерін өзгерту үшін, өзгерту құқықтары бар пайдаланушы авторизациядан өтуі қажет.

Kaspersky Security Center 13 бағдарламасында келесі функциялары іске асырылды:

- Екі қадамдық тексеру енгізілген. Басқару консоліне рұқсатсыз қатынасу қатерін төмендету үшін екі қадамдық тексеруді қосу аласыз. Бұл параметр қосулы болса, пайдаланушының есептік жазбасының параметрлерін өзгерту үшін, өзгерту құқықтары бар пайдаланушы авторизациядан өтуі қажет. Енді KES құрылғылары үшін екі қадамдық тексеруді қосуыңызға немесе өшіруіңізге болады.

- Басқару серверіне хабарларды HTTP арқылы жібере аласыз. Басқару серверінің OpenAPI құралымен жұмыс істеу үшін Python кітапханасы және анықтамалық нұсқаулық қолжетімді.

- iOS MDM серверінің сертификатының әрекет ету мерзімі өтіп кеткеннен кейін басқарылатын iOS құрылғыларын ауыстырып қосуды қамтамасыз ету үшін iOS MDM профильдерінде қолдануға арналған резервтік сертификатты шығара аласыз.

- Бірнеше қатысушысы бар бағдарламалар қалтасы бұдан былай Басқару консолінде көрсетілмейді.

Kaspersky Security Center туралы

Бұл бөлімде Kaspersky Security Center мақсаты, өзекті мүмкіндіктері мен құрамдастары, сондай-ақ Kaspersky Security Center сатып алу тәсілдері туралы ақпарат беріледі.

Онлайн анықтамада берілген ақпарат қолданбамен бірге жеткізілген құжаттарда берілген ақпараттан өзгеше болуы мүмкін; бұл жағдайда Онлайн анықтама ең дұрыс болып саналады. Онлайн-анықтамаға бағдарлама интерфейсіне кіріктірілген сілтемелер немесе құжаттамадағы сілтеме арқылы өтуге болады. Онлайн-анықтама хабарландырусыз жаңартылуы мүмкін. Қажет болса, онлайн-анықтама мен офлайн-анықтама арасында ауысуыңызға болады.

Kaspersky Security Center бағдарламасы ұйымның желісін қорғау жүйесін басқару және қызмет көрсету жөніндегі негізгі тапсырмаларды орталықтандырылған шешуге арналған. Бағдарлама, әкімшіге ұйым желісінің қауіпсіздік деңгейі туралы егжей-тегжейлі ақпаратқа қатынасуға мүмкіндік береді және Kaspersky бағдарламалары негізінде құрылған қорғаныстың барлық құрамдастарын конфигурациялауға мүмкіндік береді.

Kaspersky Security Center бағдарламасы ұйымдардың желі әкімшілеріне және ұйымдардағы құрылғыларды қорғауға жауапты қызметкерлерге арналған.

Kaspersky Security Center көмегімен сіз:

- Өзіндікұйымның желісін, сондай-ақ қашықтағы кеңселердің немесе клиенттік ұйым-клиенттердің желілерін басқару үшін Басқару серверлерінің иерархиясын қалыптастыру.

  Мұндағы *Ұйым-клиенттер* дегеніміз – провайдер антивирустық қорғанысты қамтамасыз ететін ұйымдар.

- Клиент құрылғылары жиынтығын тұтастай басқару үшін басқару топтарының иерархиясын құру.

- Kaspersky бағдарламалары негізінде құрылған антивирустық қауіпсіздік жүйесін басқару.

- Операциялық жүйелердің кескіндерін орталықтандырылған түрде жасау және оларды желі арқылы клиент құрылғыларына орналастыру, сонымен қатар Kaspersky және басқа да бағдарламалық жасақтама өндірушілерінің бағдарламаларын қашықтан орнату.

- Kaspersky және клиент құрылғыларында орнатылған басқа жеткізушілер қолданбаларын қашықтан басқарыңыз. Жаңартуларды орнату және осалдықтарды табу және түзету.

- Kaspersky бағдарламаларының лицензиялық кілттерін клиент құрылғыларына орталықтан тарату, кілттердің қолданылуын бақылау және лицензиялардың жарамдылық мерзімін ұзарту.

- Бағдарламалар мен құрылғылардың жұмысы туралы статистика мен есептер алу.

- Kaspersky бағдарламаларының жұмысындағы маңызды оқиғалар туралы хабарландырулар алу.

- Ұялы құрылғыларды басқару.

- Құрылғының қатты дискілерінде және алынбалы дискілерде сақталған ақпаратты шифрлауды және пайдаланушылардың шифрланған деректерге қатынасуын басқару.

- Ұйымның желісіне қосылған жабдықтарды түгендеу.
- Қауіпсіздік бағдарламалары карантинге немесе сақтық көшірмелеуге орналастырылған файлдармен, сондай-ақ қауіпсіздік бағдарламалары өңдеуді кейінге қалдырған файлдармен орталықтандырылған түрде жұмыс істеу.

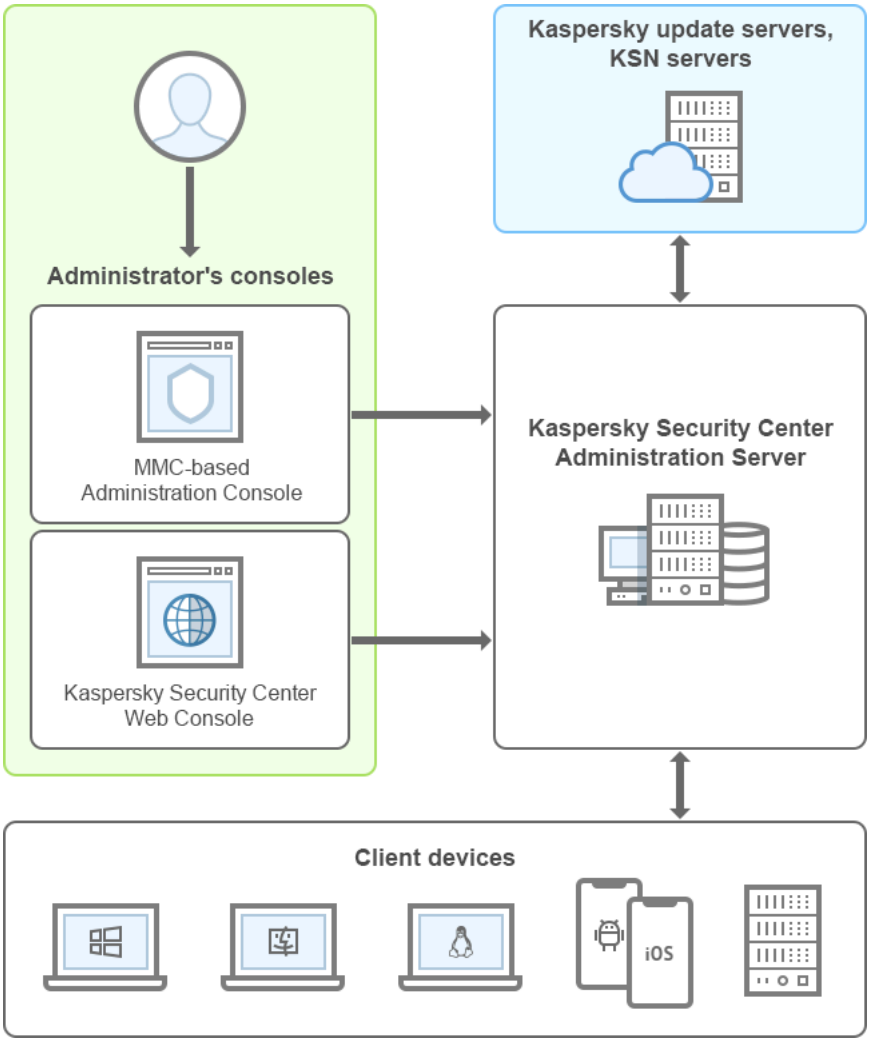
Kaspersky Security Center бағдарламасын Kaspersky арқылы (мысалы, https://www.kaspersky.ru сайтында) немесе серіктес компаниялар арқылы сатып алуға болады.

Kaspersky Security Center бағдарламасын Kaspersky арқылы сатып алсаңыз, бағдарламаны біздің сайттан жүктеп алуға болады. Бағдарламаны іске қосу үшін қажетті ақпарат төлем жасалғаннан кейін сізге электрондық пошта арқылы жіберіледі.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Бағдарлама архитектурасы

Бұл бөлімде Kaspersky Security Center құрамдастарының және олардың өзара іс-қимылының сипаттамасы бар.



Kaspersky Security Center бағдарламасы архитектурасы

Kaspersky Security Center бағдарламасы келесі негізгі құрамдастарды қамтиды:

- *Басқару консолі* (бұдан әрі – *Консоль*). Сервер мен Агенттің басқару қызметтеріне пайдаланушы интерфейсін ұсынады. Басқару консолі Microsoft Management Console (MMC) консоліне кеңейтім құрамдасы түрінде жасалған. Басқару консолі интернет арқылы қашықтағы Басқару серверіне қосылуға мүмкіндік береді.

- *Kaspersky Security Center Web Console*. Бұл Kaspersky Security Center басқаратын ұйым-клиент желісін қорғау жүйесін құруға және басқаруға арналған веб-интерфейс.

- *Kaspersky Security Center Басқару сервері* (бұдан әрі *Сервер* деп те аталады). Ұйымның желісінде орнатылған бағдарламалар және оларды басқару туралы ақпаратты орталықтандырылған сақтау функцияларын жүзеге асырады.

- *Kaspersky жаңарту серверлері*. Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

- *KSN серверлері*. Серверлерде файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы Kaspersky жедел білім базасы бар. Kaspersky Security Network Kaspersky бағдарламаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады.

- *Клиент құрылғылары*. Ұйымның клиент құрылғыларын Kaspersky Security Center қорғайды. Әрбір қорғалатын құрылғыда Kaspersky қауіпсіздік бағдарламаларының бірі орнатылуы керек.

Аппараттық және бағдарламалық талаптар

- Басқару серверіне қойылатын талаптар
- Web Console консоліне қойылатын талаптар
- Ұялы құрылғылар серверіне қойылатын талаптар
- Басқару консоліне қойылатын талаптар
- Желілік агентіне қойылатын талаптар

Мобильді құрылғыларды қорғауды орналастыру және басқаруға арналған Android және iOS нұсқаларының талаптарымен танысу үшін Kaspersky Security for Mobile Help және Kaspersky Secure Mobility Management Help анықтамалықтарын қараңыз.

Басқару серверіне қойылатын талаптар

Ең төменгі аппараттық талаптар:

- Жиілігі 1 ГГц немесе одан жоғары процессор. 64 разрядты операциялық жүйемен жұмыс істегенде процессордың минималды жиілігі 1,4 ГГц құрайды.
- Жедел жад: 4 ГБ.
- Дискідегі бос орын көлемі: 10 ГБ. Осалдықтар мен патчтарды басқару функционалдылығын қолданған кезде дискідегі бос орын кемінде 100 ГБ болуы керек.

Бұлтты ортада орналастыру үшін Басқару сервері мен дерекқор серверіне қойылатын талаптар физикалық Басқару серверімен бірдей (қанша құрылғыны басқарғыңыз келетініне байланысты).

Бағдарламалық талаптар:

- Microsoft Data Access Components (MDAC) 2.8
- Microsoft Windows DAC 6.0
- Microsoft Windows Installer 4.5

Келесі операциялық жүйелерге қолдау көрсетіледі:

Операциялық жүйеде процестер арасындағы байланыс үшін циклдік интерфейс қолжетімді болуы керек.

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 разрядты
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (орнату опциялары) (LTSB) 64 разрядты
- Windows Server 2019 Standard/Datacenter/Core 64 разрядты
- Windows Server 2022 Standard/Datacenter/Core 64 разрядты
- Windows Server 2025 Standard/Datacenter/Core 64 разрядты
- Windows Storage Server 2019 64 разрядты

Келесі виртуалдандыру платформаларына қолдау көрсетіледі:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64 разрядты
- Microsoft Hyper-V Server 2022 64 разрядты

- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

Келесі дерекқор серверлеріне қолдау көрсетіледі (басқа машинада орнатылуы мүмкін):

- Microsoft SQL Server 2016 (барлық редакциялар) 64 разрядты
- Microsoft SQL Server 2017 (барлық редакциялар) for Windows/Linux 64 разрядты
- Microsoft SQL Server 2019 (барлық редакциялар) for Windows/Linux 64 разрядты (қосымша әрекеттер керек)
- Microsoft SQL Server 2022 (барлық редакциялар) for Windows/Linux 64 разрядты
- MySQL 5.7 Community 32 разрядты/64 разрядты
- MySQL Standard Edition 8.0 (релизі 8.0.20 және одан да жоғары) 32 разрядты/64 разрядты
- MySQL Enterprise Edition 8.0 (релизі 8.0.20 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB 10.5 (жинағы 10.5.27 және одан да жоғары) 32 разрядты/64 разрядты
- MariaDB Galera Cluster 10.3 32 разрядты/64 разрядты, InnoDB қоймасы ішкі жүйесімен
- PostgreSQL 13.x 64 разрядты
- PostgreSQL 14.x 64 разрядты
- PostgreSQL 15.x 64 разрядты
- Postgres Pro 13.x Windows/Linux 64 разрядты
- Postgres Pro 14.x Windows/Linux 64 разрядты

Ақпарат пен шектеулер үшін ДҚБЖ таңдау бөлімін қараңыз.

SIEM жүйелері және ақпаратты басқарудың басқа жүйелері:

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Web Console консоліне қойылатын талаптар

Kaspersky Security Center Web Console Server сервері

Ең төменгі аппараттық талаптар:

- Процессор: 4 ядро, жиілігі 2500 МГц-тен бастап.
- Жедел жад: 8 ГБ.
- Дискідегі бос орын көлемі: 40 ГБ.

Басқару серверінің сертификатына қойылатын минималды талаптар:

- SHA-2 сертификатына қол қою алгоритмі.
- Кілттің минималды ұзындығы: 2048.

Сертификатты қайта шығару қажет болса, Kaspersky Security Center білім қорын қараңыз.

Kaspersky Security Center Web Console сервері қолдайтын операциялық жүйелер

Операциялық жүйелер. Microsoft Windows (тек 64 разрядты нұсқалар) Операциялық жүйеде процестер арасындағы байланыс үшін циклдік интерфейс қолжетімді болуы керек.	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core (орнату опциялары) (LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019
Виртуализация платформалары	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

Клиент құрылғылары

Клиент құрылғысы Kaspersky Security Center Web Console серверімен жұмыс істеу үшін тек браузерді қажет етеді.

Экранның ең төменгі ажыратымдылығы – 1366x768 пиксель.

Құрылғының аппараттық және бағдарламалық жасақтамасына қойылатын талаптар Kaspersky Security Center Web Console серверімен жұмыс істеу үшін пайдаланылатын браузердің талаптарына сәйкес келеді.

Браузерлер:

- Google Chrome 128.0.6613.120 және одан жоғары
- Microsoft Edge 128.0.2739.67 және одан жоғары
- Safari 17.6 for macOS
- Яндекс Браузері 24.7.3.1081 және одан жоғары
- Mozilla Firefox Extended Support Release 115.14.0 және одан жоғары

Ұялы құрылғылар серверіне қойылатын талаптар

iOS Mobile Device Management (iOS MDM) Ұялы құрылғылар сервері

Аппараттық талаптар:

- Жиілігі 1 ГГц немесе одан жоғары процессор. 64 разрядты операциялық жүйемен жұмыс істегенде процессордың минималды жиілігі 1,4 ГГц құрайды.
- Жедел жад: 2 ГБ.
- Дискідегі бос орын көлемі: 2 ГБ.

Microsoft Windows операциялық жүйесі (қолдау көрсетілетін операциялық жүйенің нұсқасы Басқару серверінің талаптарымен анықталады).

Басқару консоліне қойылатын талаптар

Аппараттық талаптар:

- Жиілігі 1 ГГц немесе одан жоғары процессор. 64 разрядты операциялық жүйемен жұмыс істегенде процессордың минималды жиілігі 1,4 ГГц құрайды.
- Жедел жад: 512 МБ.
- Дискідегі бос орын көлемі: 1 ГБ.

Бағдарламалық талаптар:

- Microsoft Windows операциялық жүйесі (қолдау көрсетілетін операциялық жүйенің нұсқасы басқару серверінің талаптарымен анықталады):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64 разрядты
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64 разрядты
  - Windows Server 2019 Standard/Datacenter 64 разрядты

    - Windows Server 2022 Standard/Datacenter 64 разрядты
    - Windows Server 2025 Standard/Datacenter/Core 64 разрядты
    - Windows Storage Server 2019 64 разрядты
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 осында жұмыс істейді:
    - Microsoft Windows Server 2012 R2
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Microsoft Windows Storage Server 2019
- Microsoft Windows Server 2022 Standard-та іске қосылған Microsoft Edge

Желілік агентіне қойылатын талаптар

Ең төменгі аппараттық талаптар:

- Жиілігі 1 ГГц немесе одан жоғары процессор. 64 разрядты операциялық жүйемен жұмыс істегенде процессордың минималды жиілігі 1,4 ГГц құрайды.
- Жедел жад: 512 МБ.
- Дискідегі бос орын көлемі: 1 ГБ.

Linux операциялық жүйесі бар құрылғыларға қойылатын бағдарламалық жасақтама талаптары: Perl тілі интерпретаторының 5.10 немесе одан жоғары нұсқасы орнатылуы керек.

Операциялық жүйелер. Microsoft Windows	Windows Embedded POSReady 2009, соңғы Service Pack-пен, 32 разрядты Windows Embedded 7 Standard Service Pack 1, 32 разрядты/64 разрядты Windows Embedded 8.1 Industry Pro, 32 разрядты/64 разрядты Windows 10 Enterprise 2015 LTSB, 32 разрядты/64 разрядты Windows 10 Enterprise 2016 LTSB, 32 разрядты/64 разрядты Windows 10 IoT Enterprise 2015 LTSB, 32 разрядты/64 разрядты Windows 10 IoT Enterprise 2016 LTSB, 32 разрядты/64 разрядты Windows 10 Enterprise 2019 LTSC, 32 разрядты / 64 разрядты Windows 10 IoT Enterprise 1703-нұсқа, 32 разрядты/64 разрядты Windows 10 IoT Enterprise 1709-нұсқа, 32 разрядты/64 разрядты Windows 10 IoT Enterprise 1803-нұсқа, 32 разрядты/64 разрядты Windows 10 IoT Enterprise 1809-нұсқа, 32 разрядты/64 разрядты Windows 10 20H2 IoT Enterprise 32 разрядты/64 разрядты Windows 10 21H2 IoT Enterprise 32 разрядты/64 разрядты Windows 10 IoT Enterprise 32 разрядты/64 разрядты Windows 10 IoT Enterprise 1909-нұсқа 32 разрядты/64 разрядты Windows 10 IoT Enterprise LTSC 2021 32 разрядты/64 разрядты Windows 10 IoT Enterprise 1607-нұсқа 32 разрядты/64 разрядты Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 разрядты/64 разрядты Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64 разрядты Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 разрядты Windows 8 Pro/Enterprise 32 разрядты/64 разрядты Windows 8.1 Pro/Enterprise 32 разрядты/64 разрядты Windows 7 Home/Pro/Enterprise/Ultimate Service Pack 1 32 разрядты/64 разрядты Microsoft Windows XP Professional Service Pack 2 32 разрядты/64 разрядты (тек Техникалық қолдау қызметінен сұрауға болатын Желілік агенттің 10.5.1781 нұсқасына қолдау көрсетіледі) Windows XP Professional Service Pack 3 және одан жоғары 32 разрядты (желілік агенттің 14.0.0.20023 нұсқасы қолдау көрсетеді) Windows XP Professional for Embedded Systems Service Pack 3 32 разрядты (желілік агенттің 14.0.0.20023 нұсқасы қолдау көрсетеді) Windows MultiPoint Server 2011 Standard/Premium 64 разрядты Windows Server 2003 SP1 32 разрядты/64 разрядты (тек желілік агенттің 10.5.1781 нұсқасы қолдау көрсетеді) Windows Server 2003 SP2 Standard/Enterprise 32 разрядты/64 разрядты (тек желілік агенттің 10.5.1781 нұсқасы қолдау көрсетеді) Windows Server 2003 R2 Standard/Enterprise SP2 32 разрядты/64 разрядты (тек желілік агенттің 10.5.1781 нұсқасы қолдау көрсетеді) Windows Server 2008 Standard/Enterprise/Datacenter/Foundation Service Pack 2 32 разрядты/64 разрядты Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation/ Service Pack 1 және одан да жоғары 64 разрядты

	Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64 разрядты Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 разрядты Windows Server 2016 Standard/Datacenter/Essentials/Server Core (орнату опциялары) (LTSB) 64 разрядты Windows Server 2019 Standard/Datacenter/Core 64 разрядты Windows Server 2019 RS5 Standard/Essentials 64 разрядты Windows Server 2022 Standard/Datacenter/Core 64 разрядты Windows Server 2022 21H2 Standard/Datacenter 64 разрядты Windows Server 2025 Standard/Datacenter/Core 64 разрядты Windows Storage Server 2019 64 разрядты

Операциялық жүйелер. Linux	Debian GNU/Linux 10.x (Buster) 32 разрядты/64 разрядты Debian GNU/Linux 11.x (Bullseye) 32 разрядты/64 разрядты Debian GNU/Linux 12 (Bookworm) 32 разрядты/64 разрядты Ubuntu Server 18.04 LTS (Bionic Beaver) 64 разрядты Ubuntu Server 20.04 LTS (Focal Fossa) 64 разрядты Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 разрядты Ubuntu Server 22.04 LTS ARM 64 разрядты Ubuntu Server 24.04 LTS (Noble Numbat), 64 разрядты CentOS 6.7 and later 32 разрядты CentOS 6.x (6.6 дейін), 32 разрядты/64 разрядты CentOS 7.x 64 разрядты CentOS Stream 8 64 разрядты CentOS Stream 9 64 разрядты CentOS Stream 9 ARM 64 разрядты Red Hat Enterprise Linux Server 6.x 32 разрядты/64 разрядты Red Hat Enterprise Linux Server 7.x 64 разрядты Red Hat Enterprise Linux Server 8.x 64 разрядты Red Hat Enterprise Linux Server 9.x 64 разрядты SUSE Linux Enterprise Server 12 (барлық жаңарту пакеттері) 64 разрядты SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) 64 разрядты SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) ARM, 64 разрядты openSUSE 15 64 разрядты EulerOS 2.0 SP10, 64 разрядты EulerOS 2.0 SP10 ARM 64 разрядты Astra Linux Special Edition RUSB.10015-01 (операциялық жаңарту 1.5) 64 разрядты Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.6) 64 разрядты Astra Linux Special Edition RUSB.10015-16 (1-орындау) (кезекті жаңарту 1.6) 64 разрядты Astra Linux Special Edition RUSB.10015-17 (кезекті жаңарту 1.7.3) 64 разрядты Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7) 64 разрядты Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.8) 64 разрядты Astra Linux Special Edition RUSB.10015-37 (кезекті жаңарту 7.7) 64 разрядты Astra Linux Special Edition RUSB.10152-02 (кезекті жаңарту 4.7) ARM 64 разрядты Astra Linux Common Edition (кезекті жаңарту 2.12) 64 разрядты Альт Жұмыс станциясы 10.1, 64 разрядты Альт Сервер 10.1, 64 разрядты ALT Education 10.1, 64 разрядты Альт СП Сервер 10, 32 разрядты/64 разрядты Альт СП Сервер 10 ARM, 64 разрядты Альт СП Жұмыс станциясы 10, 32 разрядты/64 разрядты Альт СП Жұмыс станциялары 10 ARM, 64 разрядты Альт Сервер 10 64 разрядты Альт Сервер 10 ARM 64 разрядты Альт Жұмыс станциясы 10 32 разрядты/64 разрядты Альт 8 СП Жұмыс станциялары (8.4) ARM, 64 разрядты Альт 8 СП Сервер (8.4) ARM, 64 разрядты Альт 8 СП Сервер (ЛКНВ.11100-01) 32 разрядты/64 разрядты Альт 8 СП Сервер (ЛКНВ.11100-02) 32 разрядты/64 разрядты Альт 8 СП Сервер (ЛКНВ.11100-03) 32 разрядты/64 разрядты Альт 8 СП Жұмыс станциясы (ЛКНВ.11100-01) 32 разрядты/64 разрядты Альт 8 СП Жұмыс станциясы (ЛКНВ.11100-02) 32 разрядты/64 разрядты Альт 8 СП Жұмыс станциясы (ЛКНВ.11100-03) 32 разрядты/64 разрядты Mageia 4 32 разрядты Oracle Linux 7 64 разрядты Oracle Linux 8 64 разрядты Oracle Linux 9 64 разрядты Linux Mint 20.x 64 разрядты

	Linux Mint 21.1 және одан жоғары 64 разрядты AlterOS 7.5 немесе одан кейінгі нұсқа, 64 разрядты ГосЛинукс IC6/7.17, 64 разрядты ГосЛинукс IC6/7.2, 64 разрядты SberOS 3.3.1 64 разрядты Platform V SberLinux OS Server (SLO) 8.8 64 разрядты Platform V SberLinux OS Server (SLO) 8.9.2 64 разрядты РЕД ОС 7.3 ARM 64 разрядты РЕД ОС 7.3 Сервер 64 разрядты РЕД ОС 7.3 Сертификатталған редакция 64 разрядты РЕД ОС 8 Сертификатталған редакция 64 разрядты ROSA Enterprise Linux Server 7.9 64 разрядты ROSA Enterprise Linux Desktop 7.9, 64 разрядты РОСА "КОБАЛЬТ" 7.9 64 разрядты РОСА "ХРОМ" 12 64 разрядты AlmaLinux 8 және одан да жоғары 64 разрядты AlmaLinux 9 және одан да жоғары, 64 разрядты Rocky Linux 8 және одан да жоғары, 64 разрядты Rocky Linux 9 және одан да жоғары, 64 разрядты Атлант, Alcyone құрастыру, 2022.02 нұсқасы, 64 разрядты МСВСфера 9.2 Сервер 64 разрядты МСВСфера 9.2 АРМ 64 разрядты СинтезМ Сервер 8.6 64 разрядты СинтезМ Клиент 8.6 64 разрядты ОСнова 2.10 64 разрядты Kylin 10 64 разрядты EMIAS 1.0 64 разрядты Amazon Linux 2 64 разрядты МосОС 15.4 Arbat, 64 разрядты OS MES (Moscow Electronic School) 64 разрядты
Операциялық жүйелер. macOS	Қолдау көрсетілетін операциялық жүйелер тізімін алу үшін Kaspersky Endpoint Security for Mac анықтамасын қараңыз.

Желілік агент үшін Intel сияқты Apple Silicon (M1) архитектурасына қолдау көрсетіледі.

Келесі виртуалдандыру платформаларына қолдау көрсетіледі:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM (ядроға негізделген виртуалды машина)

Microsoft Windows Server 2008 R2 (сервер нұсқалары) және Microsoft Windows 7 (жұмыс үстелі нұсқалары) ескі Windows нұсқаларында Желілік агент келесі функцияларды қолдамайды:

- Жаңартуларды қайта аудару (тарату нүктелері пайдаланады)
- KSN прокси (тарату нүктелері пайдаланады)
- Осалдықты сканерлеу тапсырмасы

Microsoft Windows 10 ОЖ RS4 немесе RS5 нұсқалары басқаратын құрылғыларда Kaspersky Security Center бағдарламасы тізілім есебі қосылған қалталардағы кейбір осалдықтарды анықтамауы мүмкін.

Windows 7, Windows Server 2008 немесе Windows Server 2008 R2 орнатылған құрылғыларда желілік агентті орнату алдында Windows ОЖ үшін KB3063858 қауіпсіздік жаңартуы (Windows 7 үшін қауіпсіздік жаңартуы (KB3063858)), x64 негізіндегі жүйелерге арналған Windows 7 қауіпсіздік жаңартуы (KB3063858), Windows Server 2008 үшін қауіпсіздік жаңартуы (KB3063858), Windows Server 2008 x64 Edition үшін қауіпсіздік жаңартуы (KB3063858), Windows Server 2008 R2 x64 Edition үшін қауіпсіздік жаңартуы (KB3063858) орнатылғанына көз жеткізіңіз.

Microsoft Windows XP жүйесінде Желілік агент кейбір әрекеттерді дұрыс орындамауы мүмкін.

Windows XP үшін Желілік агентті тек Microsoft Windows XP жүйесінде орнатуға немесе жаңартуға болады. Microsoft Windows XP жүйесінің қолдау көрсетілетін редакциялары және оған сай келетін Желілік агент бағдарламасының нұсқалары қолдау көрсетілетін операциялық жүйелер тізімінде берілген. Microsoft Windows XP жүйесіне арналған Желілік агент бағдарламасының қажетті нұсқасын осы беттен жүктеп алуға болады.

Желілік агенттің Kaspersky Security Center бағдарламасымен бірдей нұсқасын орнату ұсынылады.

Kaspersky Security Center желілік агенттің сол немесе одан жоғары нұсқасын толығымен қолдайды.

macOS үшін Желілік Агент осы операциялық жүйеге арналған Kaspersky қауіпсіздік бағдарламасымен бірге жеткізіледі.

Kaspersky үйлесімді бағдарламалары мен шешімдері

Kaspersky Security Center қазіргі уақытта қолдау көрсетілетін Kaspersky барлық бағдарламалары мен шешімдерін орталықтандырылған орналастыруды және басқаруды қолдайды. Төмендегі кестеде Kaspersky қандай бағдарламалары мен шешімдеріне MMC негізіндегі Басқару консолі және Kaspersky Security Center Web Console қолдау көрсететіні көрсетілген. Бағдарламалар мен шешімдердің нұсқалары туралы толық ақпарат алу үшін "Бағдарламалардың өмірлік циклі" бетін қараңыз.

Kaspersky бағдарламасының немесе шешімнің атауы	MMC негізіндегі Басқару консолінe қолдау көрсетіледі	Kaspersky Security Center Web Console қолдау көрсетіледі
Жұмыс станциялары үшін		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	—	✓
Өнеркәсіптік шешімдер үшін		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (орталықтан орналастыруға қолдау көрсетілмейді)	✓	✓
Ұялы құрылғылар үшін		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	—	✓
Файл серверлері үшін:		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Виртуалды орталар үшін		
Kaspersky Security for Virtualization Жеңіл агент	✓	✓
Kaspersky Security for Virtualization Агентсіз қорғаныс	✓	—
Мақсатты шабуылдарды анықтау үшін		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
KasperskyOS операциялық жүйесі бар құрылғылар үшін		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓
Беделдік дерекқорлар		
Kaspersky Private Security Network	—	✓

Kaspersky Security Center 15.1 лицензиялары мен мүмкіндіктері

Kaspersky Security Center бағдарламасы өзінің кейбір функциялары үшін лицензияны қажет етеді.

Төмендегі кестеде Kaspersky Security Center қандай функцияларды қамтитыны көрсетілген.

Kaspersky Security Center функцияларын пайдалану үшін басқару серверінің лицензия кілтін қосу арқылы басқару серверін белсендіру керек.

Әрбір басқару сервері үшін лицензия кілтін қолмен қосу керек.

Kaspersky Security Center лицензиялары мен мүмкіндіктері

Kaspersky Security Center функциялары	Осалдықтар мен патчтарды басқару	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
Осалдықтарды іздеу	✓	✓	✓	✓	✓	✓	✓
Патчтарды басқару	✓	–	✓	✓	–	✓	✓
Рөлге негізделген қатынасуды басқару	✓	✓	✓	✓	✓	✓	✓
Операциялық жүйелер мен бағдарламаларды орнату	✓	–	✓	✓	–	✓	✓
Ұялы құрылғыларды басқару (яғни пайдаланушылардың iOS және Android құрылғыларын басқару)	✓	✓	✓	✓	–	–	✓
AWS, Microsoft Azure немесе Google Cloud сияқты бұлтты орталарда жұмыс істеу үшін бұлтты ортаны конфигурациялау	–	–	–	–	✓	✓	–
Оқиғаларды SIEM жүйесіне экспорттау: Syslog	✓	✓	✓	✓	✓	✓	✓
Оқиғаларды SIEM жүйелеріне экспорттау: IBM ұсынған QRadar және Micro Focus ұсынған ArcSight	✓	✓	✓	✓	✓	✓	✓

Kaspersky Security Center құрамдастарының үйлесімділігі туралы ақпарат

Төмендегі кестеде Kaspersky Security Center құрамдастарының үйлесімділігі туралы ақпарат таба аласыз.

Kaspersky Security Center құрамдастарының үйлесімділігі

Құрамдас	Келесімен үйлесімді
Kaspersky Security Center 15.1 басқару сервері	• Kaspersky Security Center 15.1 басқару консолі • Kaspersky Security Center 15.1 Web Console • Kaspersky Security Center желілік агент нұсқалары: 16.3, 16.2, 16.1, 16, 15.4, 15.1, 15, 14.2, 14.
Kaspersky Security Center 15.1 Web Console	Kaspersky Security Center әкімші серверінің нұсқалары: 15.1 және 14.2
Kaspersky Security Center негізгі басқару сервері 15.1	Қосалқы басқару серверлері: • Келесі нұсқалардағы Kaspersky Security Center Windows: 14, 14.2, 15.1 • Келесі нұсқалардағы Kaspersky Security Center Linux: 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3

Құрамдас	Келесімен үйлесімді
Kaspersky Security Center қосалқы Басқару сервері 15.1	Негізгі Басқару серверлері: • Келесі нұсқалардағы Kaspersky Security Center Windows: 14, 14.2, 15.1 • Келесі нұсқалардағы Kaspersky Security Center Linux: 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3

Kaspersky Security Center басқару сервері мен Kaspersky Security Center Web Console соңғы нұсқасын пайдалану ұсынылады. Әйтпесе Kaspersky Security Center функцияларына шектеу қойылуы мүмкін. Сіз Kaspersky Security Center және Kaspersky Security Center Web Console Басқару серверін бір-бірінен тәуелсіз түрде орнатып, жаңарта аласыз. Бұл жағдайда, орнатылған Kaspersky Security Center Web Console қолданбасының нұсқасы сіз қосылатын Басқару сервері нұсқасымен үйлесімді екеніне көз жеткізіңіз:

Егер сізде Kaspersky Security Center Web Console бағдарламасының соңғы нұсқасы және Kaspersky Security Center бағдарламасының алдыңғы нұсқасы болса және домендік түпнұсқалық растама кезінде қате орын алса, қате мәтінінде стандартты хабарлама бар.

Kaspersky Security Center нұсқаларын салыстыру: Windows негізінде және Linux негізінде

Kaspersky Kaspersky Security Center бағдарламасын Windows және Linux платформаларына арналған жергілікті шешім ретінде ұсынады. Windows негізіндегі шешімде Windows құрылғысына басқару серверін орнатасыз және Linux негізіндегі шешімде Linux құрылғысына орнатуға арналған басқару серверінің нұсқасы бар. Бұл онлайн-анықтама Kaspersky Security Center Windows туралы ақпаратты қамтиды. Linux негізіндегі шешім туралы толық ақпарат алу үшін Kaspersky Security Center Linux анықтамасын қараңыз.

Төмендегі кесте Kaspersky Security Center бағдарламасының Windows негізіндегі шешімдер және Linux негізіндегі шешімдер ретінде негізгі мүмкіндіктерін салыстыруға жол ашады.

Windows негізіндегі және Linux негізіндегі Kaspersky Security Center бағдарламасының мүмкіндіктерін салыстыру

Функция немесе сипат	Kaspersky Security Center	
	Windows негізіндегі шешім	Linux негізіндегі шешім
Басқару сервері		
Деректқорларды басқару жүйесінің (ДҚБЖ) орналасуы	Жергілікті инфрақұрылымда	Жергілікті инфрақұрылымда (Microsoft SQL-ге қолдау көрсетілмейді)
Басқару серверін орнатуға арналған операциялық жүйе	Windows	Linux
Басқару серверлерінің иерархиясы	✓	✓
Виртуалды басқару серверлеріне қолдау көрсету	✓	✓
Басқару серверінің статистикасын үшінші тарап бағдарламаларына жіберу үшін SNMP пайдалану	✓	2026 жылы жүзеге асырылады
Орнату пакеттерін және басқа файлдарды жариялауға арналған веб-сервер	✓	✓
Басқару серверін бір сайтты ақауларға төзімді Windows Server кластеріне орнату	✓	—

Функция немесе сипат	Kaspersky Security Center	
	Windows негізіндегі шешім	Linux негізіндегі шешім
Ақауларға төзімді Kaspersky Security Center кластерін орналастыру	✓ Тек бір сайтты кластер	✓ Kaspersky Security Center 16.2 Linux жүйесінен бастап, географиялық таратылған ақауларға төзімді кластер қолдау табады
Басқару консолі		
Басқару консолінің түрі	MMC негізінде және веб-интерфейс	Веб-интерфейс
Веб-интерфейсі бар басқару консолін орнатуға арналған операциялық жүйе	Windows немесе Linux	Linux
Домендік түпнұсқалық растаманы пайдаланып, консольге кіру	✓	✓ 15.1-15.4 нұсқаларын қоса алғанда, бір рет кіруге қолдау көрсетілмейді
Клиент құрылғыларын және басқару топтарын басқару		
Басқарылатын құрылғылардың максималды саны (бір басқару сервері үшін)	100 000	50 000 (PostgreSQL және Postgres Pro көмегімен)
Желіде сауалнама өткізу	✓	✓ 16 нұсқасынан бастап FreeIPA және ALD Pro домен контроллеріне қолдау көрсетіледі
Windows, macOS және Linux басқаратын құрылғыларды қорғау	✓	✓
Ұялы құрылғыларды қорғау	✓ Ұялы құрылғыларды негізгі басқару	✓ MDM және Kaspersky Secure Mobility Management функциясын пайдалану (лицензия бойынша)
Виртуалды машиналарды қорғауды басқару	✓	✓
Жария бұлтты инфрақұрылымды қорғау	✓	—
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу	✓	✓ 15.3 нұсқасынан бастап
Деректерді шифрлау және қорғау	✓	✓ Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Mac бар Windows негізіндегі басқарылатын құрылғыларда
Басқару топтарындағы кластерлер мен сервер массивтеріне қолдау көрсету	✓	✓
Басқару топтары иерархиясы	✓	✓
Қосылым шлюзін тарату нүктесі ретінде демилитаризацияланған аймаққа қосу	✓ (MMC негізіндегі басқару консолі)	2026 жылы жүзеге асырылады
Пайдаланушылармен жұмыс істеу		
Пайдаланушы есептік жазбаларын жасау, есептік жазбаларды бақылау	✓	✓
Kaspersky қолданбаларын басқару		
Бағдарламалар саясаты	✓	✓
Kaspersky бағдарламаларына арналған тапсырмалар	✓	✓
Kaspersky Security Network	✓	✓
KSN прокси-сервері	✓	✓
Kaspersky Private Security Network	✓	✓
Kaspersky қолданбаларының лицензиялық кілттерін орталықтан тарату	✓	✓
Клиент құрылғыларын қашықтан диагностикалау	✓	✓

Функция немесе сипат	Kaspersky Security Center	
	Windows негізіндегі шешім	Linux негізіндегі шешім
Kaspersky бағдарламаларын автоматты түрде жаңарту	✓	✓
Аномалияларды бейімделумен басқаруды қолдау	✓	✓
Құрылғылардың қауіпсіздігін басқару	✓	✓
Пайдаланушыға бағытталған қауіпсіздікті басқару	✓	✓
Жүйелерді басқару		
Клиент құрылғыларында операциялық жүйелерді орналастыру	✓	—
Үшінші тарап лицензиясын басқару	✓	—
Басқару серверін WSUS сервері ретінде пайдалану	✓	✓ (тек Windows жаңартуының енжар іздеу режимі)
Клиент құрылғыларындағы үшінші тарап бағдарламалары бағдарламаларын басқару		
Үшінші тарап қолданбаларының жаңартуларын орнату және үшінші тарап қолданбаларындағы осалдықтарды іздеу	✓	✓
Мониторинг, есеп беру және аудит		
Нысанды тексерумен жұмыс	✓	✓
Саясат тексерістерін салыстыру	✓	2026 жылы жүзеге асырылады
Kaspersky Endpoint Detection and Response Optimum арқылы тіркелген дабылдарды көру және олармен жұмыс істеу	✓	✓
Басқарылатын құрылғыларда болған оқиғалар туралы хабарландырулар	✓	✓
Саясаттар мен тапсырмалар күйін бақылау	✓	✓
Интеграциялар		
Kaspersky Managed Detection and Response-пен біріктіру	✓	✓
SIEM жүйелерімен біріктіру	✓	✓
CEF және LEEF форматтары көмегімен оқиғаларды экспорттау	✓	✓
Дабылдарды біріктіру және Active directory, KASAP және Kaspersky TIP Sandbox арқылы жауап әрекеттерін орындау	—	✓ (15.4 нұсқасынан бастап) Kaspersky Security: Бизнеске арналған Кәсіби лицензиясында басқару серверін белсендіру, содан кейін басқарылатын қолданбаларға Kaspersky Security: Бизнеске арналған Кәсіби лицензия кілтін орналастыру керек

Kaspersky Next Expert View туралы

Kaspersky Security Center-ді жергілікті қолданба ретінде пайдалансаңыз, Kaspersky Security Center-ді, соның ішінде басқару серверін жергілікті құрылғыға орнатып, желінің қауіпсіздік жүйесін Microsoft Management Console негізіндегі басқару консолі (Kaspersky Security Center Windows-та ғана қолжетімді) немесе Kaspersky Security Center Web Console арқылы басқарасыз.

Оның орнына, сіз Kaspersky Security Center бағдарламасын бұлтты қызмет ретінде пайдалана аласыз. Бұл жағдайда, Kaspersky Security Center бағдарламасы сіз үшін Kaspersky мамандары тарапынан бұлтты ортада орнатылады және Kaspersky сізге Басқару серверіне қызмет ретінде қатысуға мүмкіндік береді. Kaspersky Next Expert View деп аталатын бұлтты қызметке негізделген Басқару консолі арқылы желі қауіпсіздігі жүйесін басқарасыз. Бұл консольде Kaspersky Security Center Web Console бағдарламасына ұқсас интерфейс бар.

Kaspersky Next Expert View интерфейсі мен құжаттамасы келесі тілдерде қолжетімді:

- Ағылшын тілі
- Француз тілі
- Неміс тілі
- Итальян тілі
- Жапон тілі
- Португал тілі (Бразилия)
- Орыс тілі
- Жеңілдетілген қытай тілі
- Испан тілі
- Испан тілі (Латын Америкасы)
- Дәстүрлі қытай тілі

Kaspersky Next Expert View және оның мүмкіндіктері туралы көбірек ақпарат Kaspersky Next Expert View құжаттамасында және Kaspersky Endpoint Security for Business құжаттамасында қолжетімді.

Kaspersky Security Center 15.1

Бұл нұсқаулықта Kaspersky Security Center 15.1 туралы ақпарат ұсынылған.

Онлайн анықтамада берілген ақпарат қолданбамен бірге жеткізілген құжаттарда берілген ақпараттан өзгеше болуы мүмкін; бұл жағдайда Онлайн анықтама ең дұрыс болып саналады. Онлайн-анықтамаға бағдарлама интерфейсіне кіріктірілген сілтемелер немесе құжаттамадағы сілтеме арқылы өтуге болады. Онлайн-анықтама хабарландырусыз жаңартылуы мүмкін. Қажет болса, онлайн-анықтама мен офлайн-анықтама арасында ауысуыңызға болады.

Негізгі ұғымдар

Бұл бөлімде Kaspersky Security Center бағдарламасына қатысты негізгі ұғымдардың егжей-тегжейлі анықтамалары бар.

Басқару сервері

Kaspersky Security Center құрамдастары клиент құрылғыларында орнатылған Kaspersky бағдарламаларын қашықтан басқаруға мүмкіндік береді.

Басқару сервері құрамдасы орнатылған құрылғылар *Басқару серверлері* (бұдан әрі - *Серверлер*) деп аталады. Басқару серверлері рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Басқару сервері құрылғыға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- "Kaspersky Security Center Басқару сервері" атауымен
- Операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен
- **LocalSystem** есептік жазбасымен немесе Басқару серверін орнату кезінде жасалған таңдауларға сәйкес пайдаланушы есептік жазбасымен

Басқару сервері келесі функцияларды орындайды:

- Басқару топтары құрылымын сақтау
- Клиент құрылғыларының конфигурациясы туралы ақпаратты сақтау
- Бағдарламалардың дистрибутивтерінің қоймаларын ұйымдастыру
- Клиент құрылғыларына бағдарламаларды қашықтан орнату және бағдарламаларды жою
- Kaspersky дерекқорлары мен бағдарлама модульдерін жаңарту
- Клиент құрылғыларындағы саясат пен тапсырмаларды басқару

- Клиент құрылғыларында болған оқиғалар туралы ақпаратты сақтау
- Kaspersky бағдарламаларының жұмысы туралы есептерді қалыптастыру
- Клиент құрылғыларына лицензиялық кілттерді тарату, кілт туралы ақпаратты сақтау
- Тапсырмалардың орындалу барысы туралы хабарландырулар жіберу (мысалы, клиент құрылғысында вирустарды анықтау)

Бағдарлама интерфейсіндегі Басқару серверлерін атау ережесі

Басқару консолі мен Kaspersky Security Center Web Console интерфейсінде Басқару серверлерінде келесі атаулар болуы мүмкін:

- Басқару сервері құрылғысының атауы, мысалы: "*құрылғы_атауы*" немесе "Басқару сервері: *құрылғы_атауы*".
- Басқару сервері құрылғысының IP мекенжайы, мысалы: "*IP_мекенжайы*" немесе "Басқару сервері: *IP_мекенжайы* ".
- Қосалқы Басқару серверлері мен виртуалды Басқару серверлерінің жалқы есімдері бар, оларды сіз виртуалды немесе қосалқы Басқару серверін негізгі Басқару серверіне қосу кезінде көрсетесіз.
- Linux басқаратын құрылғыға орнатылған Kaspersky Security Center Web Console қолданбасын пайдалансаңыз, қолданба жауап файлдарында сенімді деп көрсетілген басқару серверлерінің атауын көрсетеді.

Басқару серверіне Басқару консолінің көмегімен немесе Kaspersky Security Center Web Console көмегімен қосыла аласыз.

Басқару серверлерінің иерархиясы

Басқару серверлері иерархияны құра алады. Әрбір Басқару серверінде иерархияның әртүрлі деңгейлерінде бірнеше қосалқы Басқару серверлері (бұдан әрі - *қосалқы Серверлер*) болуы мүмкін. Қосалқы Серверлердің енгізу деңгейі шектелмейді. Бұл жағдайда, басты Серверді басқару топтарының құрамына барлық қосалқы Серверлердің клиент құрылғылары кіреді. Осылайша, компьютерлік желінің тәуелсіз аймақтарын әртүрлі Басқару серверлері басқара алады, ал оларды өз кезегінде басты Сервер басқарады.

Қосалқы Басқару серверлерінің жеке жағдайы *виртуалды Басқару серверлері* болып табылады.

Басқару серверлерінің иерархиясын келесі мақсаттар үшін қолдануға болады:

- Басқару серверіне түсетін жүктемені шектеу (желіде орнатылған бір Сервермен салыстырғанда).
- Желі ішіндегі трафикті қысқарту және қашықтағы кеңселермен жұмыс істеуді жеңілдету. Басты Сервер мен мысалы, басқа аймақтарда болуы мүмкін барлық желі құрылғылары арасында қосылым орнатудың қажеті жоқ. Желінің әр аймағында қосалқы Басқару серверлерін орнату, қосалқы Серверлердің басқару топтарында құрылғыларды тарату және қосалқы Серверлерге басты Сервермен жылдам байланыс арналары арқылы қосылуды қамтамасыз ету жеткілікті.

- Антивирустық қауіпсіздік әкімшілері арасындағы жауапкершілікті бөлу. Бұл ретте, ұйым желісінің вирусқа қарсы қауіпсіздігінің күйін орталықтандырылған басқару мен мониторингтеудің барлық мүмкіндіктері сақталады.

- Kaspersky Security Center бағдарламасын қызмет өндірушілерімен пайдалану. Провайдерге Kaspersky Security Center және Kaspersky Security Center Web Console орнату жеткілікті. Әртүрлі ұйымдардың көптеген клиент құрылғыларын басқару үшін провайдер Басқару серверлері иерархиясына (виртуалды Серверлерді қоса) қосалқы Басқару серверлерін қоса алады.

Басқару топтарының иерархиясына енгізілген әрбір құрылғыны тек бір Басқару серверіне қосуға болады. Құрылғылардың Басқару серверлеріне қосылуын өзіңіз тексеруіңіз керек. Ол үшін әртүрлі Серверлердің басқару топтарындағы желілік атрибуттар бойынша құрылғыларды іздеу функциясын пайдалануға болады.

Виртуалды Басқару сервері

Виртуалды Басқару сервері (бұдан әрі – *виртуалды Сервер*) — ұйым-клиенттің желісін басқаруға арналған Kaspersky Security Center бағдарламасының құрамдасы.

Виртуалды Басқару сервері қосалқы Басқару серверінің жеке жағдайы болып табылады және физикалық Басқару серверімен салыстырғанда келесі негізгі шектеулерге ие:

- Виртуалды Басқару сервері тек негізгі Басқару серверінің құрамында ғана жұмыс істей алады.

- Виртуалды басқару сервері жұмыс істеген кезде негізгі Басқару серверінің негізгі дерекқорын пайдаланады. Деректерді сақтық көшірмелеу және қалпына келтіру тапсырмаларына, сондай-ақ жаңартуларды тексеру және жүктеу тапсырмаларына виртуалды Басқару серверінде қолдау көрсетілмейді.

- Виртуалды сервер үшін қосалқы Басқару серверлерін (соның ішінде виртуалды) құруға қолдау көрсетілмейді.

Сонымен қатар, виртуалды Басқару серверінде келесі шектеулер бар:

- Виртуалды Серверінің сипаттары терезесінде бөлімдер жиынтығы шектеулі.

- Виртуалды Сервер басқаратын клиент құрылғыларына Kaspersky бағдарламаларын қашықтан орнату мақсатында, виртуалды Сервермен байланысу үшін клиент құрылғыларының біріне Желілік агент орнатылуы қажет. Виртуалды Басқару серверіне алғаш қосылған кезде бұл құрылғы автоматты түрде тарату нүктесі ретінде тағайындалады және виртуалды Басқару сервері мен клиент құрылғыларының қосылым шлюзі рөлін атқарады.

- Виртуалды Басқару сервері желіде тарату нүктелері арқылы ғана сауалнама өткізе алады.

- Өнімділігі бұзылған виртуалды Серверді қайта іске қосу үшін Kaspersky Security Center бағдарламасы негізгі Басқару серверін және барлық виртуалды Серверлерді қайта іске қосады.

- Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Виртуалды Сервер әкімшісі осы виртуалды Сервердің шеңберінде барлық құқықтарға ие.

Ұялы құрылғылардың сервері

Ұялы құрылғылар сервері – бұл ұялы құрылғыларға қатынасуға мүмкіндік беретін және оларды Басқару консолі арқылы басқаруға мүмкіндік беретін Kaspersky Security Center құрамдасы. Ұялы құрылғы сервері ұялы құрылғылар туралы ақпарат алады және олардың профильдерін сақтайды.

Kaspersky Security Center Ұялы құрылғылар сервері ретінде iOS MDM серверін қамтиды. Бұл Ұялы құрылғы сервері Apple Push Notifications (APNs) серверін қолдайтын ұялы құрылғыларды басқару үшін қолданылады.

Kaspersky Security Center Ұялы құрылғылар серверлері келесі нысандарды басқаруға мүмкіндік береді:

- Бөлек ұялы құрылғыны.
- Бірнеше ұялы құрылғыны.
- Серверлер кластеріне бір уақытта қосылған бірнеше ұялы құрылғыны. Серверлер кластеріне қосылу кезінде, осы кластерде орнатылған Ұялы құрылғылар сервері Басқару консолінде сервер ретінде көрсетіледі.

Веб-сервер

Kaspersky Security Center *Web Server* (бұдан әрі – *Веб-сервер*) – бұл Басқару серверінің құрамында орнатылатын Kaspersky Security Center құрамдасы. Веб-сервер жеке орнату пакеттерін, iOS MDM профильдерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды желі арқылы беруге арналған.

Жасау кезінде, жеке орнату пакеті Веб-серверде автоматты түрде жарияланады. Автономды пакетті жүктеу сілтемесі, жасалған автономды орнату пакеттерінің тізімінде көрсетіледі. Қажет болса, автономды пакетті жариялауды болдырмауға немесе оны Веб-серверде қайта жариялауға болады.

Жасаған кезде, пайдаланушының ұялы құрылғысына арналған iOS MDM профилі Веб-серверде дәл солай автоматты түрде жарияланады. Жарияланған профиль пайдаланушының ұялы құрылғысына сәтті орнатылғаннан кейін, Веб-серверден автоматты түрде жойылады.

Ортақ қатынасы бар қалта, құрылғылары Басқару сервері басқаратын барлық пайдаланушыларға қолжетімді ақпаратты орналастыру үшін пайдаланылады. Егер пайдаланушының ортақ қатынасы бар қалтаға тікелей қатынасу мүмкіндігі болмаса, оған Веб-сервер арқылы сол қалтадан ақпарат жіберуге болады.

Пайдаланушыларға Веб-сервер арқылы ортақ қатынасы бар қалтадан ақпарат беру үшін әкімші ортақ қатынасы бар қалтада салынған public қалтасын жасап, оған ақпаратты орналастыруы керек.

Пайдаланушыға ақпарат беру үшін сілтеме синтаксисі келесідей:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

мұндағы

- `<Web Server name>` – Kaspersky Security Center Веб-серверінің атауы.
- `<HTTPS port>` – әкімші белгілеген Веб-сервер HTTPS порты. HTTPS портын Басқару сервері сипаттары терезесінің **Веб-сервер** бөлімінде белгілеуге болады. Әдепкі бойынша 8061-порт орнатылған.
- `<object>` – пайдаланушы үшін қатынасу мүмкіндігін ашуды қажет ететін салынған қалта немесе файл.

Әкімші қалыптастырылған сілтемені пайдаланушыға кез келген ыңғайлы тәсілмен, мысалы, электрондық пошта арқылы жібере алады.

Алынған сілтеме бойынша пайдаланушы өзіне арналған ақпаратты жергілікті құрылғыға жүктей алады.

Желілік агент

Басқару сервері мен құрылғылар арасындағы өзара іс-қимылды *Желілік агент* – Kaspersky Security Center құрамдасы қамтамасыз етеді. Желілік агент Kaspersky бағдарламаларының жұмысын басқару Kaspersky Security Center көмегімен орындалатын барлық құрылғыларға орнатылуы қажет.

Желілік агент құрылғыларға келесі атрибуттар жиынтығы бар қызмет ретінде орнатылады:

- "Kaspersky Security Center Желілік агенті" атауымен
- Операциялық жүйені іске қосу кезінде автоматты түрде іске қосу түрімен
- LocalSystem есептік жазбасы көмегімен

Желілік агент орнатылған құрылғы *басқарылатын құрылғы* немесе *құрылғы* деп аталады.

Желілік агент Windows, Linux немесе Mac операциялық жүйесі басқаратын құрылғыға орнатылуы мүмкін. Құрамдасты келесі жолдармен белсендіруге болады:

- Басқару сервері қоймасындағы орнату пакеті (Басқару сервері орнатылуы керек)
- Орнату пакеті Kaspersky веб-серверлерінде орналасқан

Желілік агентті Басқару сервері орнатылған құрылғыларға орнатудың қажеті жоқ, өйткені Желілік агенттің серверлік нұсқасы Басқару серверімен бірге автоматты түрде орнатылады.

Желілік агентті іске қосатын процестің атауы, – *klnagent.exe*.

Желілік агент басқарылатын құрылғыларды Басқару серверімен синхрондайды. Синхрондау кезеңін (*мерзімді сигнал*) 10 000 басқарылатын құрылғыға 15 минутқа тең етіп белгілеу ұсынылады.

Басқару топтары

Басқару тобы (бұдан әрі *топ* деп те аталады) – бұл топтың құрылғыларын біртұтас Kaspersky Security Center ретінде басқару мақсатында қандай да бір белгі бойынша біріктірілген басқарылатын құрылғылар жиынтығы.

Басқару тобындағы барлық басқарылатын құрылғылар үшін төмендегілер белгіленеді:

- Бағдарламалардың жұмысының бірыңғай параметрлері – топтық саясаттар көмегімен.
- Барлық бағдарламалардың бірыңғай жұмыс режимі – белгілі бір параметрлер жиынтығы бар топтық тапсырмаларды құру арқылы. Топтық тапсырмалар мысалдарына: жалпы орнату пакетін жасау және орнату, бағдарлама дерекқорлары мен модульдерін жаңарту, құрылғыны талап бойынша тексеру және тұрақты қорғанысты қосу кіреді.

Басқарылатын құрылғы тек бір басқару тобының құрамына кіре алады.

Басқару серверлері мен басқару топтары үшін кез келген тіркеме деңгейі бар иерархиялар жасауға болады. Иерархияның бір деңгейінде қосалқы және виртуалды Басқару серверлері, топтар және басқарылатын құрылғылар орналасуы мүмкін. Құрылғыларды физикалық түрде жылжытпай, бір топтан екінші топқа ауыстыруға болады. Мысалы, кәсіпорын қызметкері бухгалтер лауазымынан әзірлеуші лауазымына ауысса, сіз сол қызметкердің құрылғысын "Бухгалтерлер" басқару тобынан "Әзірлеушілер" басқару тобына ауыстыра аласыз. Осылайша әзірлеушілер үшін қажетті қолданба параметрлері құрылғыға автоматты түрде жіберіледі.

Басқарылатын құрылғы

Басқарылатын құрылғы – желілік агент орнатылған Windows, Linux немесе macOS басқаратын құрылғы немесе Kaspersky қауіпсіздік қолданбасы орнатылған мобильдік құрылғы. Сіз мұндай құрылғыларды, құрылғыларда орнатылған бағдарламаларға арналған тапсырмалар мен саясаттардың көмегімен басқара аласыз. Сондай-ақ, сіз басқарылатын құрылғыларға арналған есептерді құрастыра аласыз.

Сіз тарату нүктесі мен қосылым шлюзі функцияларын орындайтын басқарылатын ұялы емес құрылғыны конфигурациялай аласыз.

Құрылғы тек бір Басқару серверінің басқаруымен болуы мүмкін. Бір Басқару сервері ұялы құрылғыларды қоса алғанда, 100 000-ға дейінгі құрылғыларға қызмет көрсете алады.

Тағайындалмаған құрылғы

Тағайындалмаған құрылғы – бірден-бір басқару тобына қосылмаған желідегі құрылғы. Сіз тағайындалмаған құрылғылармен әрекеттерді орындай аласыз, мысалы, оларды басқару топтарына көшіре аласыз, оларға бағдарламалар орната аласыз.

Желіде жаңа құрылғы анықталған кезде, ол **Тағайындалмаған құрылғылар** басқару тобына орналастырылады. Құрылғыларды анықтаған сәтте басқару топтары бойынша автоматты түрде тарату ережелерін конфигурациялауға болады.

Әкімшінің жұмыс станциясы

Әкімшінің жұмыс станциясы — Басқару консолі орнатылған немесе сіз Kaspersky Security Center Web Console веб-консолімен жұмыс істеу үшін пайдаланатын құрылғы. Осы құрылғылардан әкімшілер клиент құрылғыларында орнатылған Kaspersky бағдарламаларын қашықтан орталықтандырылған басқаруды жүзеге асыра алады.

Басқару консолін орнату нәтижесінде сіздің құрылғыда Басқару консолін іске қосу белгішесі пайда болады. Оны **Бастау** → **Бағдарламалар** → **Kaspersky Security Center** мәзірінде табыңыз.

Әкімшінің жұмыс станцияларының саны шектелмейді. Әрбір әкімші жұмыс станциясынан желідегі бірнеше Басқару серверлерінің басқару топтарын бірден басқаруға болады. Әкімшінің жұмыс станциясын кез келген иерархия деңгейіндегі Басқару серверіне (физикалық және виртуалды) қосуға болады.

Әкімшінің жұмыс станциясын клиент құрылғысы ретінде басқару тобы құрамына қосуға болады.

Кез келген Сервердің басқару топтарында бір құрылғы бір уақытта Басқару серверінің клиенті де, Басқару сервері де және әкімшінің жұмыс станциясы да бола алады.

Басқару плагині

Басқару консолі арқылы Kaspersky бағдарламаларын басқару арнайы құрамдастың – *басқару плагинінің* көмегімен жүзеге асырылады. Kaspersky Security Center көмегімен басқаруға болатын әрбір Kaspersky бағдарламасының құрамына басқару плагині кіреді.

Басқару консоліндегі бағдарламаны басқару плагинінің көмегімен келесі әрекеттерді орындауға болады:

- бағдарлама саясаттары мен параметрлерін, сондай-ақ осы бағдарламаның тапсырма параметрлерін жасау және өңдеу;
- бағдарламаның тапсырмалары, оның жұмысындағы оқиғалар, сондай-ақ клиент құрылғыларынан алынған бағдарламаның жұмыс статистикасы туралы ақпарат алу.

Сіз басқару плагиндерін Kaspersky Техникалық қолдау қызметі веб-сайтынан жүктеп ала аласыз.

Басқару веб-плагиндері

Басқару веб-плагиндері – Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалары тарапынан қашықтан басқару үшін қолданылатын арнайы құрамдас. Басқару веб-плагині *басқару плагині* деп те аталады. Басқару плагині Kaspersky Security Center Web Console бағдарламасы мен Kaspersky белгілі бір бағдарламасы арасындағы интерфейс болып табылады. Басқару плагині көмегімен бағдарлама үшін тапсырмалар мен саясаттарды конфигурациялауға болады.

Сіз басқару веб-плагиндерін Kaspersky Техникалық қолдау қызметі веб-сайтынан жүктеп ала аласыз.

Басқару плагині келесі мүмкіндіктерді ұсынады:

- Бағдарламаның тапсырмалары мен параметрлерін жасауға және өзгертуге арналған интерфейс.
- Kaspersky бағдарламалары мен құрылғыларды қашықтан орталықтандырылған түрде конфигурациялау үшін саясаттар мен саясаттар профильдерін жасауға арналған өзгертуге арналған интерфейс.
- Бағдарламалар қалыптастырған оқиғаларды беру.
- Бағдарламаның оқиғалары мен жедел деректерін, сондай-ақ клиент құрылғысынан алынған статистиканы көрсетуге арналған Kaspersky Security Center Web Console функциялары.

Саясаттар

Саясат — басқару тобы мен оның ішкі топтарына қолданылатын Kaspersky қолданбасы параметрлерінің жиынтығы. Kaspersky бағдарламаларының бірнешеуін басқару тобының құрылғыларына орната аласыз. Kaspersky Security Center бағдарламасы басқару тобындағы Kaspersky бағдарламасының әрқайсысы үшін бір саясаттан ұсынады. Саясаттың келесі күйлерінің бірі бар (төмендегі кестені қараңыз):

Саясат күйі

Күй	Сипаттамасы
Белсенді	Бұл, құрылғыға қатысты қолданылатын ағымдағы саясат. Kaspersky бағдарламасы үшін әрбір басқару тобында тек бір саясат белсенді болуы мүмкін. Kaspersky бағдарламасының белсенді саясаты параметрлерінің мәндері құрылғыға қатысты қолданылады.
Белсенді емес	Қазіргі уақытта құрылғыға қатысты қолданылмайтын саясат.
Автономды пайдаланушылар үшін	Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.

Саясаттар келесі ережелер бойынша әрекет етеді:

- Бір бағдарлама үшін түрлі мәндері бар бірнеше саясатты конфигурациялауға болады.
- Бір бағдарлама үшін тек бір саясат белсенді болуы мүмкін.
- Белгілі бір оқиға туындаған кезде, белсенді емес саясатты белсендіре аласыз. Мысалы, вирустық шабуыл кезеңінде күшейтілген антивирустық қорғаныс үшін параметрлерді қоса аласыз.
- Саясаттың еншілес саясаттары болуы мүмкін.

Сіз вирустық шабуыл сияқты төтенше жағдайларға дайындалу үшін саясатты қолдана аласыз. Мысалы, USB флеш-дискілері арқылы шабуыл орын алса, флеш-дискілерге қатынасуға тыйым салатын саясатты іске қосуға болады. Бұл жағдайда, ағымдағы белсенді саясат автоматты түрде белсенді емес болады.

Көптеген саясаттарды қолдамау үшін, мысалы, әртүрлі жағдайларда бірнеше параметрлерді ғана өзгерту қажет болғанда, сіз саясат профильдерін қолдана аласыз.

Саясат профилі – саясат параметрлерін алмастыратын аталған саясат параметрлері ішкі жиынтығы. Саясат профилі басқарылатын құрылғының тиімді параметрлерін қалыптастыруға әсер етеді. *Тиімді параметрлер* – қазіргі уақытта құрылғыға қатысты қолданылатын саясат параметрлері, саясат профилі параметрлері және жергілікті бағдарлама параметрлері жиынтығы.

Саясат профильдері келесі ережелер бойынша жұмыс істейді:

- Саясат профилі белгіленген белсендіру шарты туындаған кезде күшіне енеді.
- Саясат профильдері саясат параметрлерінен ерекшеленетін параметр мәндерін қамтиды.
- Саясат профилін белсендіру кезінде басқарылатын құрылғының тиімді параметрлері өзгереді.
- Саясатта ең көбі 100 профиль болуы мүмкін.

Саясат профильдері

Әртүрлі басқару топтары үшін бір саясаттың бірнеше көшірмесін жасау қажеттілігі туындауы мүмкін; осы саясаттардың параметрлерін орталықтан өзгерту қажеттілігі де туындауы ықтимал. Бұл көшірмелер бір немесе екі параметрде ерекшеленуі мүмкін. Мысалы, ұйымдағы барлық бухгалтерлер бірдей саясаттың басқаруымен жұмыс істейді, бірақ аға бухгалтерлерге USB флеш-дискілерін пайдалануға рұқсат етіледі, ал кіші бухгалтерлерге рұқсат етілмейді. Бұл жағдайда, басқару топтарының иерархиясы арқылы құрылғыларға саясаттарды қолдану ыңғайсыз болуы мүмкін.

Бір саясаттың бірнеше көшірмесін жасауды болдырмау үшін Kaspersky Security Center бағдарламасы *саясат профильдерін* жасауға мүмкіндік береді. Саясат профильдері, бір басқару тобындағы құрылғылардың әртүрлі саясат параметрлері болуы үшін қажет.

Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер басқарылатын құрылғыда әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды. Профильді белсендіру кезінде құрылғыда бастапқыда әрекет еткен "негізгі" саясат параметрлері өзгереді. Бұл параметрлер профильде көрсетілген мәндерді қабылдайды.

Тапсырмалар

Kaspersky Security Center *тапсырмаларды* құру және іске қосу арқылы құрылғыларда орнатылған Kaspersky қауіпсіздік бағдарламаларының жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Бағдарлама үшін басқару плагині орнатылған жағдайда ғана тапсырма жасай аласыз.

Тапсырмалар Басқару серверінде және құрылғыларда орындалуы мүмкін.

Басқару серверінде орындалатын тапсырмалар:

- Есептерді автоматты түрде жеткізу
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу
- Басқару сервері деректерінің сақтық көшірмесін жасау
- Дерекқорларға қызмет көрсету
- Windows Update жаңартуларын синхрондау
- Эталондық құрылғының операциялық жүйесінің кескінінің орнату пакетін жасау

Құрылғыларда тапсырмалардың келесі түрлері орындалады:

- *Жергілікті тапсырмалар* – нақты құрылғыда орындалатын тапсырмалар.

  Жергілікті тапсырмаларды тек әкімші Басқару консолі арқылы ғана емес, қашықтағы құрылғының пайдаланушысы да өзгерте алады (мысалы, қауіпсіздік бағдарламасының интерфейсінде). Егер жергілікті тапсырманы басқарылатын құрылғыда әкімші де, пайдаланушы да бір уақытта өзгерткен болса, онда әкімші енгізген өзгерістер басым болып күшіне енеді.

- *Топтық тапсырмалар* – бұл аталған топтың барлық құрылғыларында орындалатын тапсырмалар.

  Егер тапсырманың сипаттарында басқаша көрсетілмесе, топтық тапсырма аталған топтың ішкі топтарына да таралады. Топтық тапсырмалар (міндетті емес) осы топқа және ішкі топтарға орналастырылған қосалқы және виртуалды Басқару серверлеріне қосылған құрылғыларда да жұмыс істейді.

- *Глобалдық тапсырмалар* – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.

Әр бағдарлама үшін сіз топтық тапсырмалардың, глобалдық тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Құрылғыдағы тапсырмаларды іске қосу тек осы тапсырмалар жасалған бағдарлама іске қосылған жағдайда ғана орындалады.

Тапсырмаларды орындау нәтижелері Microsoft Windows және Kaspersky Security Center, орталықтандырылған түрде Басқару серверінде де, жергілікті түрде әрбір құрылғыда да оқиғалар журналдарында сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Тапсырманың әрекет ету ауқымы

Тапсырма ауқымы — тапсырма орындалатын құрылғылар жинағы. Тапсырма ауқымының келесі түрлері бар:

- *Жергілікті тапсырма* ауқымы – құрылғының өзі.
- *Басқару серверінің тапсырмасы* ауқымы – Басқару сервері.
- *Топтық тапсырма* ауқымы – топқа кіретін құрылғылардың тізбесі.

Глобалдық тапсырма жасаған кезде оның ауқымын анықтаудың келесі әдістерін қолдануға болады:

- Қажетті құрылғыларды қолмен көрсету.

  Құрылғының мекенжайы ретінде сіз IP мекенжайын (немесе IP аралығын), NetBIOS немесе DNS атауын пайдалана аласыз.

- Құрылғылар тізімін қосылатын құрылғылар мекенжайлары тізбесін қамтитын TXT пішіміндегі файлдан құрылғылар тізімін импорттау (әр мекенжай бөлек жолда орналасуы тиіс).

  Егер құрылғылар тізімі файлдан импортталса немесе қолмен қалыптастырылса, ал құрылғылар атауы бойынша анықталса, онда тізімге ақпараты Басқару серверінің дерекқорына әлдеқашан қосылған құрылғылар ғана қосылуы мүмкін. Деректер, осы құрылғыларды қосу кезінде немесе құрылғыларды анықтау нәтижесінде дерекқорға енгізілуі тиіс.

- Құрылғы таңдауларын көрсету.

  Уақыт өте келе, тапсырманың әрекет ету ауқымы, таңдауға кіретін құрылғылардың жиынтығы қалай өзгеретіндігіне байланысты өзгеріп отырады. Құрылғыны таңдауы құрылғы атрибуттары негізінде, соның ішінде құрылғыда орнатылған бағдарламалық жасақтама негізінде, сондай-ақ құрылғыға белгіленген тегтер негізінде құрылуы мүмкін. Құрылғыны таңдауы тапсырманың әрекет ету ауқымын белгілеудің ең икемді тәсілі болып саналады.

  Құрылғы таңдаулары үшін тапсырмаларды кесте бойынша іске қосуды әрқашан Басқару сервері орындайды. Мұндай тапсырмалар Басқару серверімен байланысы жоқ құрылғыларда іске қосылмайды. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғыларда тікелей іске қосылады және құрылғы мен Басқару сервері арасындағы байланыстың болуына тәуелді емес.

  Құрылғылар таңдауына арналған тапсырмалар құрылғының жергілікті уақыты бойынша емес, Басқару серверінің жергілікті уақыты бойынша іске қосылады. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғының жергілікті уақыты бойынша іске қосылады.

Саясат пен бағдарламаның жергілікті параметрлерінің өзара байланысы

Сіз саясаттардың көмегімен топтың құрамына кіретін барлық құрылғылар үшін бағдарламаның жұмыс параметрлерінің бірдей мәндерін орната аласыз.

Топтағы жеке құрылғылар үшін саясат белгілеген параметрлердің мәндерін бағдарламаның жергілікті параметрлері арқылы қайта анықтауға болады. Бұл жағдайда, сіз өзгертуге саясат тыйым салмаған параметрлердің мәндерін ғана орната аласыз (параметр құлыпталмаған).

Клиент құрылғысындағы бағдарлама қолданатын параметрдің мәні, саясаттағы параметрде құлыптың (🔒) болуымен анықталады:

- Егер параметрді өзгертуге тыйым салынса, барлық клиент құрылғылары бірдей саясатпен белгіленген мәнді пайдаланады.

- Егер тыйым салынбаған болса, онда әрбір клиент құрылғысында бағдарлама саясатта көрсетілгеннен гөрі жергілікті параметр мәнін пайдаланады. Бұл жағдайда, параметрдің мәні бағдарламаның жергілікті параметрлері арқылы өзгеруі мүмкін.

Осылайша, клиент құрылғысында тапсырманы орындау кезінде бағдарлама екі түрлі жолмен берілген параметрлерді қолданады:

- егер саясатта параметрді өзгертуге тыйым салынбаған болса, тапсырма параметрлері және бағдарламаның жергілікті параметрлері арқылы;

- егер саясатта параметрді өзгертуге тыйым салынған болса, топтың саясаты арқылы.

Бағдарламаның жергілікті параметрлері саясат параметрлеріне сәйкес саясатты бірінші рет қолданғаннан кейін өзгереді.

Тарату нүктесі

Тарату нүктесі (бұған дейін "жаңартулар агенті" деп аталып келген) — жаңартуларды тарату, қолданбаларды қашықтан орнату, желідегі құрылғылар туралы ақпарат алу үшін қолданылатын желілік агент орнатылған құрылғы. Тарату нүктелері жаңартуларды таратуды тездетеді және Басқару серверінің ресурстарын босатуға мүмкіндік береді.

Тарату нүктесі ретінде пайдаланылатын құрылғыда орнатылған желілік агент мүмкіндіктері мен пайдалану жағдайлары операциялық жүйеге байланысты әртүрлі.

Тарату нүктесі келесі функцияларды орындауы мүмкін:

- Басқару серверінен алынған файлдарды топтың клиент құрылғыларына тарату (соның ішінде UDP протоколы арқылы кеңінен тарататын таратылым арқылы).

  Тарату нүктелері арқылы тасымалдауға болатын файлдар тізімі мыналарды қамтиды:

  - Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдері
  - Үшінші тарап бағдарламалық жасақтамасының жаңартулары
  - Орнату пакеттері
  - Басқару серверін WSUS сервері ретінде пайдаланған кездегі Windows жаңартулары

  Жаңартулар Басқару серверінен де, Kaspersky жаңарту серверлерінен де алынуы мүмкін. Соңғы жағдайда, тарату нүктесі үшін жаңарту тапсырмасы жасалуы тиіс. macOS басқаруындағы тарату нүктелері Kaspersky жаңарту серверлерінен жаңартуларды жүктеп ала алмайды.

  > macOS операциялық жүйесі бар құрылғылар *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының әрекет ету ауқымында болса, онда тапсырма Windows операциялық жүйесі бар құрылғылардың барлығында сәтті аяқталса да, *Сәтсіз аяқталды* мәртебесімен аяқталады.

  > Құрылғыға тағайындалған барлық тарату нүктелері ақаулы болған кезде, құрылғы жаңартуларды (антивирустық дерекқорлар мен патчтарды) және орнату пакеттерін алмайды.

- Саясаттар мен топтық тапсырмаларды UDP протоколы бойынша кеңінен тарататын таратылым арқылы тарату.

- Басқару тобы құрылғылары үшін Басқару серверімен қосылым шлюзі рөлін орындау.

  Топтың басқарылатын құрылғылары мен Басқару сервері арасында тікелей қосылым жасау мүмкін болмаса, онда тарату нүктесін осы топтың Басқару серверімен қосылым шлюзі ретінде тағайындауға болады. Бұл жағдайда, басқарылатын құрылғылар қосылым шлюзіне, ол болса Басқару серверіне қосылады.

  Қосылым шлюзі ретінде жұмыс істейтін тарату нүктесінің болуы басқарылатын құрылғыларды Басқару серверіне тікелей қосуды жоққа шығармайды. Қосылым шлюзі қолжетімді болмаса, ал Басқару серверіне тікелей қосылу мүмкін болса, басқарылатын құрылғылар тікелей Серверге қосылады.

- Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

- Үшінші тарап бағдарламалары мен Kaspersky бағдарламаларын қашықтан орнатуды тарату нүктесі операциялық жүйесінің құралдары көмегімен орындау. Тарату нүктесі клиент құрылғыларына орнатуды Желілік агентсіз орындауы мүмкін екендігіне назар аударыңыз.

  Бұл функция, Басқару сервері тікелей қатынаса алмайтын желілерде орналасқан клиент құрылғыларына Желілік агенттің орнату пакеттерін қашықтан жіберуге мүмкіндік береді.

- Kaspersky Security Network (KSN) желісінде қатысатын прокси-сервер рөлінде әрекет ету.

  Құрылғы KSN прокси-сервері рөлін орындауы үшін KSN прокси-серверін тарату нүктесі жағында қосуға болады. Бұл жағдайда, құрылғыда KSN прокси-сервері (ksnproxy) қызметі іске қосылады.

Файлдарды Басқару серверінен тарату нүктесіне жіберу HTTP протоколы арқылы немесе SSL қосылымының қолданылуы конфигурацияланған болса – HTTPS протоколы арқылы жүзеге асырылады. HTTP немесе HTTPS протоколын қолдану, SOAP протоколын қолданумен салыстырғанда трафикті қысқарту арқасында аса жоғары өнімділікті қамтамасыз етеді.

Желілік агенті орнатылған құрылғыларды, тарату нүктелері тарапынан әкімші өз қолымен немесе Басқару сервері автоматты түрде тағайындауы мүмкін. Көрсетілген басқару топтары үшін тарату нүктелерінің толық тізімі, тарату нүктелерінің тізімі бар есепте көрсетіледі.

Тарату нүктесінің әрекет ету аумағы, ол әкімші болып тағайындалған басқару тобы, сондай-ақ оның барлық тіркеме деңгейлеріндегі ішкі топтар болып саналады. Басқару топтарының иерархияларында бірнеше тарату нүктесі тағайындалған болса, басқарылатын құрылғының Желілік агенті иерархия бойынша ең жақын тарату нүктесіне қосылады.

Тарату нүктелерінің әрекет ету аумағы, желілік орналасу болуы мүмкін. Желілік орналасу, тарату нүктесі жаңартуларды тарататын арнайы құрылғыларды қолмен қалыптастыру мақсатымен қолданылады. Желілік орналасуды анықтау, тек Windows операциялық жүйесінің басқаруындағы құрылғылар үшін ғана қолжетімді.

Тарату нүктелерін Басқару сервері автоматты түрде тағайындайтын болса, онда Сервер тарату нүктелерін басқару топтары бойынша емес, кеңінен тарататын домендер бойынша тағайындайды. Бұл, кеңінен тарататын домендер белгілі болғаннан кейін орын алады. Желілік агент өзінің ішкі желісінің басқа да Желілік агенттерімен хабар алмасады және өзі туралы ақпарат пен басқа да Желілік агенттер туралы қысқаша ақпаратты Басқару серверіне жібереді. Осы ақпарат негізінде, Басқару сервері Желілік агенттерді кең тарататын домендер бойынша топтастыра алады. Кең тарататын домендер Басқару серверіне басқару топтарындағы Желілік агенттердің 70%-дан астамы сұрастырылғаннан кейін белгілі болады. Басқару сервері кеңінен тарататын домендерді екі сағат сайын сұрастырып тұрады. Тарату нүктелері кеңінен тарататын домендер бойынша тағайындалғаннан кейін, оларды басқару топтары бойынша қайтадан тағайындауға болмайды.

Әкімші тарату нүктелерін қолмен тағайындаса, оларды басқару топтарына немесе желілік орындарға тағайындауға болады.

Белсенді қосылым профилі бар Желілік агенттер кеңінен тарататын доменді анықтауға қатыспайды.

Kaspersky Security Center әрбір Желілік агентке басқа мекенжайлармен қиылыспайтын көп мекенжайлы IP таратылымының бірегей мекенжайын белгілейді. Соның арқасында, мекенжайлардың қиылысуына байланысты желіге түсетін жүктеменің артуының алдын алуға болады.

Желінің бір аумағында немесе басқару тобында екі немесе одан да көп тарату нүктесі тағайындалса, олардың бірі белсенді тарату нүктесі болып, қалғандары резервтік болады. Белсенді тарату нүктесі жаңартулар мен орнату пакеттерін тікелей Басқару серверінен жүктеп алады, ал резервтік тарату нүктелері жаңартуларды алу үшін тек белсенді тарату нүктесіне жүгінеді. Бұл жағдайда, файлдар Басқару серверінен тек бір рет жүктеліп, одан кейін тарату нүктелері арасында бөлінеді. Белсенді тарату нүктесі қандай да бір себептермен қолжетімді емес болып қалса, резервтік тарату нүктелерінің бірі белсенді болып тағайындалады. Басқару сервері тарату нүктесін автоматты түрде резервтік деп тағайындайды.

Тарату нүктесі күйі (*Белсенді*/*Резервтік*) klnagchk утилитасы есебінде жалауша түрінде көрсетіледі.

Тарату нүктесінің жұмыс істеуі үшін дискіде кемінде 4 ГБ бос орын керек. Тарату нүктесінің дискісіндегі бос орын көлемі 2 ГБ-тан кем болса, Kaspersky Security Center орталығы *Ескерту* маңыздылық деңгейіне ие қауіпсіздік мәселесін жасайды. Қауіпсіздік мәселесі құрылғы сипаттарында **Қауіпсіздік мәселелері** бөлімінде жарияланады.

Тарату нүктесі бар құрылғыда қашықтан орнату тапсырмалары жұмыс істеген кезде, қосымша бос диск кеңістігі қажет болады. Бос диск кеңістігі, орнатылатын орнату пакеттерінің барлығының өлшемінен үлкен болуы тиіс.

Тарату нүктесі бар құрылғыда жаңартуларды (патчтарды) орнату және осалдықты түзету тапсырмасы жұмыс істеген кезде, қосымша бос диск кеңістігі қажет болады. Бос дискі кеңістігі, орнатылатын патчтардың барлығының өлшемінен кемінде екі есе үлкен болуы тиіс.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Қосылым шлюзі

Қосылым шлюзі – ерекше режимде жұмыс істейтін Желілік агент. Қосылым шлюзі басқа Желілік агенттерінен қосылымдарды қабылдайды және оларды Сервермен орнатылған өзінің қосылымы арқылы Басқару серверіне туннельдейді. Әдеттегі Желілік агенттен айырмашылығы, қосылым шлюзі Басқару серверімен байланыс орнатпайды, тек Басқару серверінен қосылымдарды күтеді.

Қосылым шлюзі 10 000 құрылғыдан қосылымдарды қабылдай алады.

Қосылым шлюздерін пайдаланудың екі нұсқасы бар:

- Демилитаризацияланған аймаққа (DMZ) қосылым шлюзін орнату ұсынылады. Автономды құрылғыларда орнатылған басқа Желілік агенттер үшін қосылым шлюзі арқылы Басқару серверіне қосылуды арнайы конфигурациялау қажет.

  Қосылу шлюзі Желілік агенттерден Басқару серверіне берілетін деректерді өзгертпейді немесе өңдемейді. Қосылым шлюзі бұл деректерді буферге жазбайды, сондықтан Желілік агенттен деректерді қабылдай алмайды, содан кейін оларды Басқару серверіне жібере алмайды. Желілік агент Басқару серверіне қосылым шлюзі арқылы қосылуға тырысса, бірақ қосылым шлюзі Басқару серверіне қосыла алмаса, Желілік агент мұны қолжетімді емес Басқару сервері ретінде қабылдайды. Барлық деректер Желілік агентте қала береді (қосылым шлюзінде емес).

  Қосылым шлюзі басқа қосылым шлюзі арқылы Басқару серверіне қосыла алмайды. Бұл дегеніміз, Желілік агент бір уақытта қосылым шлюзі бола алмайды және Басқару серверіне қосылу үшін қосылым шлюзін қолдана алмайды.

Барлық қосылым шлюздері Басқару сервері сипаттарындағы тарату нүктелерінің тізіміне енгізілген.

- Сондай-ақ, желідегі қосылым шлюздерін пайдалануға болады. Мысалы, автоматты түрде тағайындалатын тарату нүктелері өзінің әрекет ету ауқымында дәл солай қосылым шлюздеріне айналады. Алайда, ішкі желіде қосылым шлюздері айтарлықтай артықшылықтар бермейді. Олар Басқару сервері қабылдаған желілік қосылымдардың санын азайтады, бірақ кіріс деректерінің көлемін азайтпайды. Қосылым шлюздері болмаса да, барлық құрылғылар Басқару серверіне қосыла алады.

Негізгі орнату сценарийі

Негізгі сценарийді орындай отырып, сіз Басқару серверін орналастыра аласыз, сонымен қатар желі құрылғыларына Желілік агент пен қауіпсіздік бағдарламаларын орната аласыз. Сіз бұл сценарийді бағдарламамен танысу үшін де, одан әрі жұмыс істеу мақсатымен бағдарламаны орнату үшін де пайдалана аласыз.

Kaspersky Security Center бағдарламасын орнату келесі қадамдарды қамтиды:

1. Дайындық
2. Басқару сервері бар құрылғыда Kaspersky Security Center және Kaspersky қауіпсіздік бағдарламаларын орнату
3. Клиент құрылғыларында Kaspersky қауіпсіздік бағдарламаларын қашықтан орналастыру

Kaspersky Security Center-ді бұлтты ортада орналастыру және провайдерлер үшін Kaspersky Security Center-ді орналастыру анықтаманың тиісті бөлімдерінде сипатталған.

Басқару серверін орнатуға кемінде бір сағат, ал сценарийді толығымен орындауға кемінде бір жұмыс күнін бөлу ұсынылады. Kaspersky Security Center басқару сервері рөлін атқаратын құрылғыда Kaspersky Security for Windows Server немесе Kaspersky Endpoint Security сияқты қауіпсіздік қолданбасын орнату да ұсынылады.

Сценарий аяқталғаннан кейін, ұйымның желісінде қорғаныс келесі тәсілмен орналастырылады:

- Басқару сервері үшін ДҚБЖ орнатылады.
- Kaspersky Security Center Басқару сервері орнатылады.
- Барлық қажетті саясаттар мен тапсырмалар жасалады, сонымен қатар әдепкі бойынша саясат пен тапсырма параметрлері конфигурацияланады.
- Басқарылатын құрылғыларда қауіпсіздік бағдарламалары (мысалы, Kaspersky Endpoint Security for Windows) және Желілік агент орнатылады.
- Басқару топтары құрылады (бәлкім, иерархияға біріктірілген).
- Қажет болса, ұялы құрылғылардың қорғанысы орналастырылады.
- Қажет болса, тарату нүктелері тағайындалады.

Kaspersky Security Center орнату кезең-кезеңімен жүзеге асырылады:

Дайындық.

1. **Қажетті файлдарды алу**

   Kaspersky Security Center үшін лицензиялық кілт (белсендіру коды) немесе Kaspersky қауіпсіздік бағдарламалары үшін лицензия кілттері (белсендіру кодтары) бар екеніне көз жеткізіңіз.

   Жеткізушіден алынған мұрағатты ашыңыз. Бұл мұрағатта лицензиялық кілттер (KEY пішіміндегі файлдар), белсендіру кодтары және осы лицензиялық кілттердің әрқайсысы белсендіре алатын Kaspersky бағдарламаларының тізімі бар.

   Егер сіз Kaspersky Security Center-ді қолданып көргіңіз келсе, Kaspersky веб-сайтынан отыз күндік сынақ нұсқасын ала аласыз.

   Kaspersky Security Center құрамына кірмейтін Kaspersky қауіпсіздік бағдарламаларын лицензиялау туралы толық ақпаратты осы бағдарламалардың құжаттамасынан таба аласыз.

2. **Ұйымның қорғаныс құрылымын таңдау**

   Kaspersky Security Center құрамдастарымен танысыңыз. Ұйымыңызға ең қолайлы қорғаныс құрылымы мен желі конфигурациясын таңдаңыз. Желі конфигурациясы мен байланыс арналарының өткізу қабілеттілігіне сүйене отырып, Басқару серверлерінің қанша санын пайдалану керектігін және егер сіз таратылған желімен жұмыс жасасаңыз, оларды кеңселерге қалай орналастыру керектігін анықтаңыз.

   Әртүрлі жұмыс жағдайында оңтайлы өнімділікке қол жеткізу және сақтау үшін желідегі құрылғылардың санын, желі топологиясын және сізге қажет Kaspersky Security Center функциялары жиынтығын ескеріңіз (толығырақ Kaspersky Security Center өлшеу нұсқаулығын қараңыз).

   Ұйымыңызда Басқару сервері иерархиясы қолданылады ма екенін анықтаңыз. Бұл үшін барлық клиент құрылғыларына бір Басқару серверімен қызмет көрсету мүмкін бе және мақсатқа сай келеді ме, әлде Басқару серверлерінің иерархиясын құру қажет пе екенін түсіну керек. Сондай-ақ, сізге желісін қорғағыңыз келетін кәсіпорынның ұйымдық құрылымымен сәйкес келетін Басқару серверлерінің иерархиясын құру қажет болуы мүмкін.

   Мобильдік құрылғылар қорғанысын қамтамасыз ету қажет болса, iOS MDM серверін реттеуге арналған дайындық әрекеттерін орындаңыз.

   Басқару серверлері ретінде пайдалану үшін, сондай-ақ Басқару консолін орнату үшін таңдаған құрылғылардың аппараттық және қолданбалық құрал талаптарына сәйкес келетініне көз жеткізіңіз.

3. **Пайдаланушы сертификаттарын пайдалануға дайындық**

   Ұйымыңыздың жалпыға ортақ кілт инфрақұрылымы (PKI) сізден белгілі бір сенімді сертификаттау орталығы (CA) шығарған пайдаланушы сертификаттарын пайдалануды талап етсе, осы сертификаттарды дайындаңыз және олардың барлық талаптарға сай екеніне көз жеткізіңіз.

4. **Kaspersky Security Center лицензиялауға дайындық**

   Егер сіз Ұялы құрылғыларды басқаруды, SIEM жүйелерімен біріктіруді қолдайтын және/немесе Жүйелік басқаруды қолдайтын Kaspersky Security Center нұсқаны пайдалануды жоспарласаңыз, бағдарламаны лицензиялау үшін кілт файлы немесе белсендіру коды бар екеніне көз жеткізіңіз.

5. **Басқарылатын қауіпсіздік бағдарламаларын лицензиялауға дайындық**

   Қорғанысты орналастыру кезінде сізге Kaspersky ұйымына Kaspersky Security Center арқылы басқарғыңыз келетін қолданбаларға белсенді лицензиялық кілттер беру қажет болады (басқару үшін қолжетімді қауіпсіздік қолданбаларының тізімін қараңыз). Қауіпсіздік бағдарламаларының әрқайсысын лицензиялау туралы толығырақ осы бағдарламалардың құжаттамасынан оқи аласыз.

6 Басқару сервері мен ДҚБЖ аппараттық конфигурациясын таңдау

Желідегі құрылғылар санын ескере отырып, ДҚБЖ және Басқару сервері үшін аппараттық конфигурацияны жоспарлаңыз.

7 ДҚБЖ таңдау

ДҚБЖ таңдау кезінде Басқару серверіне қызмет көрсететін басқарылатын құрылғылардың санын ескеріңіз. Егер сіздің желіңізде 10 000-нан аз құрылғы болса және олардың санын көбейтуді жоспарламасаңыз, сіз тегін SQL Express немесе MySQL ДҚБЖ таңдап, оны Басқару сервері бар бір құрылғыға орната аласыз. Сіз 20 000-ға дейінгі құрылғыны басқаруға мүмкіндік беретін MariaDB ДҚБЖ таңдай аласыз. Егер сіздің желіңізде 10 000-нан астам құрылғы болса (немесе сіз желіні осындай құрылғылар санына дейін кеңейтуді жоспарласаңыз), ақылы SQL ДҚБЖ таңдап, оны бөлек құрылғыға орналастырған жөн. Ақылы ДҚБЖ бірнеше Басқару серверлерімен, ал тегін ДҚБЖ тек біреуімен ғана жұмыс істей алады.

Егер сіз SQL Server серверін таңдасаңыз, онда дерекқорда сақталған деректерді MySQL, MariaDB немесе Azure SQL ДҚБЖ-ға тасымалдауға болады. Деректерді тасымалдау үшін деректердің сақтық көшірмесін жасап, оларды жаңа ДҚБЖ-да қалпына келтіріңіз.

> Егер сіз MSSQL 2019 нұсқасын таңдасаңыз, CU12 немесе одан кейінгі жинақталған патчын пайдалануыңыз керек. Бұл сізге орын алуы мүмкін қателер мен жүйенің шамадан тыс жүктелуін болдырмауға мүмкіндік береді.

8 ДҚБЖ орнату және дерекқор жасау

ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар туралы көбірек біліңіз және ДҚБЖ орнатыңыз.

Орнату алдында қолдау көрсетілетін ДҚБЖ таңдаңыз. Мысалы, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL немесе MariaDB таңдауға болады.

Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

MariaDB, MySQL, PostgreSQL немесе Postgres Pro орнатсаңыз, онда ДҚБЖ дұрыс жұмыс істеуін қамтамасыз ету үшін ұсынылатын параметрлерді қолданыңыз.

ДҚБЖ параметрлерін жазып алыңыз және сақтаңыз, өйткені олар Басқару серверін орнатқан кезде сізге қажет болады. Бұл параметрлерге SQL серверінің атауы, SQL серверіне қосылу үшін порт нөмірі, SQL серверіне кіру үшін есептік жазба атауы және құпиясөз кіреді.

> Егер сіз PostgreSQL немесе Postgres Pro ДҚБЖ орнатуды шешсеңіз, суперпайдаланушының құпиясөзін енгізгеніңізге көз жеткізіңіз. Егер құпиясөз көрсетілмесе, Басқару сервері дерекқорға қосылмауы мүмкін.

Әдепкі бойынша, Kaspersky Security Center инсталляторы Басқару сервері туралы ақпаратты орналастыру үшін дерекқор жасайды, бірақ сіз оны құрудан бас тартып, басқа дерекқор пайдалана аласыз. Бұл жағдайда, дерекқордың жасалғанына, оның атауын білетініңізге, ал Басқару сервері сол дерекқорға қатынаса алатын есептік жазбада ол үшін db_owner рөлі болатындығына көз жеткізіп алыңыз.

Қажет болса, ақпарат алу үшін ДҚБЖ әкімшісіне хабарласыңыз.

9 Порттарды конфигурациялау

Сіз таңдаған қорғаныс құрылымына сәйкес құрамдастардың өзара әрекеттесуі үшін қажетті порттардың барлығы ашық екеніне көз жеткізіңіз.

Егер интернеттен Басқару серверіне қатынас ұсыну қажет болса, порттар мен қосылым параметрлерін желі конфигурациясына қарай конфигурациялаңыз.

10 Есептік жазбаларды тексеру

Kaspersky Security Center Басқару серверін сәтті орнату және құрылғыларда қорғанысты орналастыру үшін жергілікті әкімші құқықтарыңыздың бар екеніне көз жеткізіңіз. Клиент құрылғыларына Желілік агентті орнату үшін осы құрылғыларда жергілікті әкімші құқықтары қажет. Желілік агент орнатылғаннан кейін, сіз оның көмегімен құрылғы әкімшісінің құқықтары бар есептік жазбаны пайдаланбай, бағдарламаларды құрылғыларға қашықтан орната аласыз.

Әдепкі бойынша, Kaspersky Security Center инсталляторы Басқару серверін орнату үшін таңдалған құрылғыда үш жергілікті есептік жазбаны жасайды, олардың атынан Kaspersky Security Center Басқару сервері мен қызметтері іске қосылады:

- KL-AK-*: Басқару сервері қызметінің есептік жазбасы;
- NT Service/KSC*: Басқару сервері құрамындағы басқа қызметтерге арналған есептік жазба;
- KlPxeUser: операциялық жүйелерді орналастыруға арналған есептік жазба.

Басқару сервері қызметтері мен басқа қызметтер үшін есептік жазбалар жасаудан бас тартуға болады. Мұның орнына, сіз Басқару серверін істен шығуға төзімді кластерге орнатуды жоспарласаңыз немесе басқа себеппен жергілікті есептік жазбалардың орнына домен есептік жазбаларын пайдалануды жоспарласаңыз, домен есептік жазбалары сияқты бар есептік жазбаларды пайдалана аласыз. Бұл жағдайда, Kaspersky Security Center Басқару сервері мен қызметтерін іске қосуға арналған есептік жазбалар артықшылықты емес екеніне ДҚБЖ-не қатынасу үшін қажетті құқықтарға ие екеніне көз жеткізіңіз (Егер сіз алдағыда операциялық жүйелерді құрылғыларда Kaspersky Security Center құралдарымен орналастыруды жоспарласаңыз, есептік жазбаларды жасаудан бас тартпаңыз.)

Басқару сервері бар құрылғыда Kaspersky Security Center және Kaspersky қауіпсіздік бағдарламаларын орнату

1. **Басқару серверін, Басқару консолін, Kaspersky Security Center Web Console және қауіпсіздік бағдарламаларына арналған басқару плагиндерін орнату**

   Kaspersky Security Center бағдарламасын Kaspersky сайтынан жүктеп алыңыз. Толық пакетті, тек Kaspersky Security Center Web Console немесе тек Басқару консолін жүктеп алуға болады.

   Басқару серверін сіз таңдаған құрылғыға (немесе бірден артық Басқару серверін пайдалануды жоспарласаңыз, құрылғыларға) орнатыңыз. Басқару серверін стандартты немесе таңдаулы орнатуды таңдауға болады. Басқару серверімен бірге Басқару консолі орнатылады. Басқару серверін домен контроллеріне емес, бөлектенген серверге орнату ұсынылады.

   Kaspersky Security Center бағдарламасымен танысқыңыз келсе, мысалы, оның жұмысын сіздің желіңіздің шағын бөлігінде сынағыңыз келсе, стандартты орнату тәсілі ұсынылады. Стандартты орнату кезінде сіз тек дерекқор параметрлерін конфигурациялайсыз. Сондай-ақ, сіз тек Kaspersky бағдарламалары үшін әдепкі бойынша орнатылған басқару плагиндерінің жиынтығын ғана орната аласыз. Kaspersky Security Center бағдарламасымен жұмыс істеп көрсеңіз және стандартты орнатудан кейін сізге қажетті барлық параметрлерді қалай конфигурациялау керектігін білсеңіз, стандартты орнатуды пайдалана аласыз.

   Kaspersky Security Center параметрлерін, мысалы, ортақ қатынасы бар қалтаға апаратын жолды, есептік жазбаларды және Басқару серверіне қосылу порттары және дерекқор параметрлерін конфигурациялауды жоспарласаңыз, онда таңдаулы орнату тәсілі ұсынылады. Таңдаулы орнату, Kaspersky бағдарламаларын басқару плагиндерінің қайсысы орнатылатынын көрсетуге мүмкіндік береді. Қажет болса, сіз таңдаулы орнатуды тыныш режимде іске қоса аласыз.

   Басқару серверімен бірге Басқару консолі және Желілік агенттің серверлік нұсқасы да орнатылады. Kaspersky Security Center Web Console орнатуды да таңдауға болады.

   Қажет болса, желі арқылы Басқару серверін басқару үшін Басқару консолі мен Kaspersky Security Center Web Console веб-консолін әкімшінің жұмыс орнына дербес орнатуға болады.

2. **Бастапқы конфигурациялау және лицензиялау**

   Басқару серверін орнату аяқталғаннан кейін, Басқару серверіне алғаш рет қосылған кезде Бағдарламаны жылдам іске қосу шебері автоматты түрде іске қосылады. Сіздің талаптарыңызға сәйкес Басқару серверін бастапқы конфигурациялауды орындаңыз. Бағдарламаны жылдам іске қосу кезеңінде, шебер қорғанысты орналастыру үшін қажетті әдепкі бойынша параметрі бар саясат пен тапсырманы жасайды. Бұл параметрлер сіздің ұйымыңыздың қажеттіліктері үшін оңтайлы болмауы мүмкін. Қажет болса, саясат пен тапсырма параметрлерін өзгертуге болады (Ұйым-клиент желісінде қорғанысты конфигурациялау, Сценарий: желі қорғанысын конфигурациялау).

   Егер сіз Базалық функционалдылықтан тыс функционалдылықты пайдалануды жоспарласаңыз, бағдарламаны лицензия бойынша белсендіріңіз. Мұны бағдарламаны жылдам іске қосу шебері қадамдарының бірінде орындай аласыз.

3. **Басқару серверін орнатудың сәтті орындалуын тексеру**

   Алдыңғы қадамдарды сәтті орындағаннан кейін, Басқару сервері орнатылып, әрі қарай жұмыс істеуге дайын.

   Басқару консолі жұмыс істеп тұрғанына және Консоль арқылы Басқару серверіне қосылуға болатындығына көз жеткізіңіз. Басқару серверінде Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы (консоль шежіресінің **Тапсырмалар** қалтасында) және Kaspersky Endpoint Security үшін саясат (консоль шежіресінің **Саясаттар** қалтасында) бар екеніне де көз жеткізіңіз.

   Тексеру аяқталғаннан кейін, төмендегі қадамдарға өтіңіз.

Клиент құрылғыларында Kaspersky қауіпсіздік бағдарламаларын қашықтан орналастыру

1. **Желідегі құрылғыларды табу**

   Бұл қадам бағдарламаны жылдам іске қосу шеберіне кіреді. Сіз құрылғыларды табуды қолмен де іске қоса аласыз. Нәтижесінде, Kaspersky Security Center Басқару сервері желіде тіркелген барлық құрылғылардың мекенжайлары мен атауларын алады. Алдағыда, Kaspersky Security Center көмегімен табылған құрылғыларға Kaspersky және басқа өндірушілердің бағдарламаларын орната аласыз. Kaspersky Security Center құрылғыларды анықтауды үнемі іске қосады, сондықтан желіде жаңа құрылғылар пайда болса, олар автоматты түрде анықталады.

2. **Желідегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнату**

   Ұйымның желісінде қорғанысты орналастыру (Ұйымның желісінде қорғанысты конфигурациялау, Сценарий: Желі қорғанысын конфигурациялау) Желілік агент пен қауіпсіздік бағдарламаларын (мысалы, Kaspersky Endpoint Security) Басқару сервері құрылғыларды анықтау барысында анықтаған құрылғыларға орнатуды көздейді.

   Қауіпсіздік бағдарламалары құрылғыларды вирустардан және/немесе басқа қауіп төндіретін бағдарламалардан қорғайды. Желілік агент құрылғының Басқару серверімен байланысын қамтамасыз етеді. Желілік агенттің параметрлері әдепкі бойынша автоматты түрде конфигурацияланады.

   Қажет болса, Желілік агентті интерактивті емес (тыныш) режимде, жауаптар файлымен немесе онсыз да орнатуға болады.

   Желідегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнатпас бұрын, бұл құрылғылардың қолжетімді (яғни қосулы) екеніне көз жеткізіңіз. Желілік агентті виртуалды машиналарға, сондай-ақ физикалық құрылғыларға орната аласыз.

   Қауіпсіздік бағдарламалары мен Желілік агентті қашықтан немесе жергілікті орнатуға болады.

   Қашықтан орнату – қорғанысты орналастыру шебері көмегімен сіз қауіпсіздік бағдарламасын (мысалы, Kaspersky Endpoint Security for Windows) және Желілік агентті ұйымның желісінде Басқару сервері анықтаған құрылғыларға қашықтан орната аласыз. Әдетте, қашықтан орнату тапсырмасы көптеген желілік құрылғылар үшін қорғанысты сәтті орналастырады. Алайда, мысалы, құрылғы өшірілген болса немесе басқа себеппен қолжетімді болмаса, ол кейбір құрылғыларда қатені қайтаруы мүмкін. Бұл жағдайда, құрылғыға қолмен қосылып, жергілікті орнатуды пайдалану ұсынылады.

Жергілікті орнату – қашықтан орнату тапсырмасы арқылы қорғанысты қолдану мүмкін болмаған желілік құрылғыларда қолданылады. Мұндай құрылғыларда қорғанысты орнату үшін, осы құрылғыларда жергілікті іске қосу мақсатында жеке орнату пакетін жасаңыз.

Linux және macOS операциялық жүйелері бар құрылғыларға Желілік агентті орнату, сәйкесінше Kaspersky Endpoint Security for Linux және Kaspersky Endpoint Security for Mac құжаттамасында сипатталған. Linux және macOS операциялық жүйелерінің басқаруымен жұмыс істейтін құрылғылар Windows операциялық жүйесіне қарағанда осал болып саналса да, оларға да қауіпсіздік бағдарламаларын орнату ұсынылады.

Орнатқаннан кейін, қауіпсіздік бағдарламасы басқарылатын құрылғыларға орнатылғанына көз жеткізіңіз. Бұл үшін Kaspersky бағдарламалық жасақтамасының нұсқалары туралы есепті іске қосып, оның нәтижелерімен танысыңыз.

3. **Лицензиялық кілттерді клиент құрылғыларына тарату**

   Осы құрылғыларда басқарылатын қауіпсіздік бағдарламаларын белсендіру үшін лицензиялық кілттерді клиент құрылғыларына таратыңыз.

4. **Ұялы құрылғылар қорғанысын конфигурациялау**

   Бұл қадам бағдарламаны жылдам іске қосу шеберіне кіреді.

   Корпоративтік ұялы құрылғыларды басқару үшін, қажетті дайындық қадамдарын орындап, Ұялы құрылғыларды басқаруды орналастырыңыз.

5. **Басқару топтарының құрылымын жасау**

   Кейбір жағдайларда қорғанысты желі құрылғыларында оңтайлы түрде орналастыру үшін құрылғыларды ұйымның ұйымдық құрылымын ескере отырып, басқару топтарына бөлу қажет болуы мүмкін. Құрылғыларды топтар бойынша тарату немесе құрылғыларды қолмен тарату үшін жылжыту ережелерін жасауға болады. Басқару топтары үшін топтық тапсырмаларды тағайындауға, саясаттардың әрекет ету ауқымын анықтауға және тарату нүктелерін тағайындауға болады.

   Барлық басқарылатын құрылғылар тиісті басқару топтары бойынша таратылғанына және желіңізде тағайындалмаған құрылғылардың қалмағанына көз жеткіңіз.

6. **Тарату нүктелерін тағайындау**

   Kaspersky Security Center, басқару топтарына тарату нүктелерін автоматты түрде тағайындайды, бірақ қажет болған жағдайда оларды қолмен тағайындауға болады. Тарату нүктелерін Басқару серверіне жүктемені азайту үшін үлкен желілерде, сондай-ақ Басқару серверіне өткізу қабілеті төмен арналармен біріктірілген құрылғыларға немесе құрылғылар тобына қатынасуды ұсыну үшін таратылған құрылымы бар желілерде пайдалану ұсынылады. Тарату нүктелері ретінде Linux және Windows басқаруымен жұмыс істейтін құрылғыларды пайдалануға болады.

Kaspersky Security Center қолданатын порттар

Төмендегі кестелерде басқару сервері және клиент құрылғылары пайдаланатын әдепкі порттар көрсетілген. Қаласаңыз, әдепкі бойынша порт нөмірлерін өзгерте аласыз.

Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт, Microsoft SQL Server үшін 1433-порт немесе PostgreSQL және Postgres Pro үшін 5432-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
8060	klcsweb	TCP	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Әдепкі бойынша порт нөмірін Басқару консолiндегі Басқару сервері сипаттары терезесінің **Веб-сервер** бөлімінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз. Бұл порт міндетті емес. Қауіпсіздік мақсатында 8061 TCP портын пайдалану ұсынылады.
8061	klcsweb	TCP (TLS)	Клиент құрылғыларына жарияланған орнату пакеттерін беру	Орнату пакеттерін жариялау. Әдепкі бойынша порт нөмірін Басқару консолiндегі Басқару сервері сипаттары терезесінің **Веб-сервер** бөлімінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
13000	klserver	TCP (TLS)	Желілік агенттерден және қосалқы Басқару серверлерінен қосылымдарды қабылдау; басты Серверден қосылымдарды қабылдау үшін қосалқы серверлерде де қолданылады (мысалы, егер қосалқы Сервер демилитаризацияланған аймақта болса)	Клиенттік құрылғыларды және бағынышты Басқару серверлерді басқару. Қосылым порттарын конфигурациялау кезінде желілік агенттерден қосылымдарды қабылдайтын әдепкі порт санын өзгертуге болады; басқару консолінде немесе Kaspersky Security Center Web Console-де басқару серверлерінің иерархиясын жасаған кезде, қосымша басқару северлерінен қосылымдарды қабылдайтын әдепкі порт санын өзгертуге болады.
13000	klserver	UDP	Желілік агенттерден құрылғыларды өшіру туралы ақпарат қабылдау	Клиент құрылғыларын басқару. Әдепкі бойынша порт нөмірін Басқару консолiндегі желілік агент саясаты параметрлерінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
13291	klserver	TCP (TLS)	Басқару консолінен Басқару серверіне қосылымдар қабылдау	Басқару серверін басқару. Әдепкі бойынша порт нөмірін Басқару консолiндегі Басқару сервері сипаттары терезесінде өзгерте аласыз.
13299	klserver	TCP (TLS)	Kaspersky Security Center Web Console веб-консолінен Басқару серверіне қосылымдар алу; Басқару серверінен OpenAPI арқылы қосылымдар алу	Kaspersky Security Center Web Console, OpenAPI. Әдепкі порт нөмірін басқару консолiндегі басқару серверінің сипаттар терезесінде (**Басқару серверіне қосылу параметрлері** бөлімі → **Қосылу порттары** ішкі бөлімі) немесе басқару консолі немесе Kaspersky Security Center Web Console ішінде басқару серверлерінің иерархиясын жасаған кезде өзгертуге болады.
14000	klserver	TCP	Желілік агенттерден қосылымдар қабылдау	Клиент құрылғыларын басқару. Сіз әдепкі бойынша порт нөмірін Kaspersky Security Center орнатқанда қосылу порттарын конфигурациялау кезінде немесе клиент құрылғысын Басқару серверіне қолмен қосу кезінде өзгерте аласыз. Бұл порт міндетті емес. Қауіпсіздік мақсатында 13000 TCP портын пайдалану ұсынылады.
13111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	TCP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.
15111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	UDP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.
17000	klactprx	TCP (TLS)	Басқарылатын құрылғылардан бағдарламаларды белсендіру үшін қосылымдарды қабылдау (ұялы құрылғылардан басқа)	Ұялы емес құрылғылар белсендіру кодтарының көмегімен Kaspersky бағдарламаларын белсендіру үшін қолданатын белсендіру прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
17100 (ұялы құрылғыларды басқарсаңыз ғана)	klactprx	TCP (TLS)	Ұялы құрылғылардан қолданбаларды белсендіру үшін қосылымдарды қабылдау	Ұялы құрылғыларға арналған белсендіру прокси-сервері. Әдепкі бойынша порт мәндерін Басқару сервері сипаттары терезесінде өзгерте аласыз.
19170	klserver	HTTPS (TLS)	klsctunnel утилитасы көмегімен басқарылатын құрылғылармен байланысты туннельдеу	Kaspersky Security Center Web Console арқылы басқарылатын құрылғыларға қашықтан қосылу. Әдепкі порт нөмірін басқару консоліндегі басқару серверінің сипаттар терезесінде ғана өзгертуге болады (**Басқару серверіне қосылу параметрлері** бөлімі → **Қосылу порттары** ішкі бөлімі → **Kaspersky Security Center Web Console үшін RDP портын ашу** опциясы).
13292 (ұялы құрылғыларды басқарсаңыз ғана)	klserver	TCP (TLS)	Ұялы құрылғылардан қосылымдар қабылдау	Ұялы құрылғыларды басқару. Әдепкі бойынша порт нөмірін Басқару консоліндегі Басқару сервері сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
13294 (ұялы құрылғыларды басқарсаңыз ғана)	klserver	TCP (TLS)	UEFI деңгейлі қорғанысты құрылғылардан қосылымдар қабылдау	UEFI деңгейлі қорғанысты клиент құрылғыларын басқару. Әдепкі порт нөмірін басқару консоліндегі немесе Kaspersky Security Center Web Console ішіндегі басқару серверінің сипаттар терезесінде (**Басқару серверіне қосылу параметрлері** бөлімі → **Қосылу порттары** ішкі бөлімі) мобильдік құрылғыларды байланыстырған кезде немесе кейінірек өзгертуге болады.
13296	klserver	TCP (TLS)	Prometheus үшін Kaspersky Security Center көрсеткіштерін жариялау	Prometheus кейінірек алатын Kaspersky Security Center көрсеткіштерін жариялау. Метрикаларды мына сілтемеден көре аласыз: https://<адрес_сервера>:13296/metrics. <сервер_мекенжайы> өрісінде басқару серверіңіздің IP мекенжайын немесе домен атын көрсетіңіз. Әдепкі бойынша порт нөмірін Басқару консоліндегі Басқару сервері сипаттары терезесінде өзгерте аласыз.
30522, 30523 (localhost интерфейсіндегі порттар)	klnagent	TCP	Қолданба жаңартуларын Желілік агенттен жергілікті орнатылған Kaspersky қолданбаларына FileTransferBridge компоненті арқылы тасымалдау	Kaspersky бағдарламалары үшін жаңартуларды алатын Басқару сервер құрылғысы.

Төмендегі кестеде iOS MDM серверінде қолданылатын порт көрсетілген (мобильдік құрылғыларды басқарсаңыз ғана).

iOS MDM сервері қолданатын порт

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
443	kliosmdmservicesrv	TCP (TLS)	iOS ұялы құрылғыларынан қосылымдар қабылдау	Ұялы құрылғыларды басқару. iOS MDM серверін орнату кезінде әдепкі бойынша порт нөмірін өзгерте аласыз.

Төмендегі кестеде Kaspersky Security Center Web Console Server пайдаланатын порт көрсетілген. Бұл, Басқару сервері орнатылған дәл сол құрылғы, не болмаса басқа құрылғы болуы мүмкін.

Kaspersky Security Center Web Console Server қолданатын порт

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
8080	Node.js: серверлік JavaScript	TCP (TLS)	Браузерден қосылымдар қабылдау және Kaspersky Security Center Web Console веб-консолiне жiберу	Kaspersky Security Center Web Console. Windows немесе Linux басқаратын құрылғыда Kaspersky Security Center Web Console орнату кезінде әдепкі бойынша порт нөмірін өзгерте аласыз. Kaspersky Security Center Web Console веб-консолін ALT Linux операциялық жүйесі бар құрылғыға орнатып жатсаңыз, онда 8080-порттан ерекшеленетін портты көрсету керек, себебі 8080-портты операциялық жүйе қолданады.

Төмендегі кестеде желілік агент орнатылған басқарылатын құрылғыларда қолданылатын порт көрсетілген.

Желілік агент қолданатын порттар

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
15000	klnagent	UDP	Басқару серверінен немесе тарату нүктесінен желілік агенттерге берілетін сигналдарды басқару	Клиент құрылғыларын басқару. Әдепкі бойынша порт нөмірін Басқару консолiндегi желілік агент саясаты параметрлерінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
15000	klnagent	UDP бойынша кеңінен тарататын таратылым	Дәл сол кеңінен тарататын домендегі басқа Желілік агенттер туралы деректер алу (бұдан әрі деректер Басқару серверіне жіберіледі)	Жаңартулар мен орнату пакеттерін жеткізу.
15001	klnagent	UDP	Тарату нүктелерінен көп мекенжайлы сұрауларды алу (қолданылса)	Тарату нүктесінен жаңартулар мен орнату пакеттерін алу. Әдепкі бойынша порт нөмірін Басқару консолiндегi тарату нүктесі сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
30522, 30523 (localhost интерфейсіндегі порттар)	klnagent	TCP	FileTransferBridge компоненті арқылы Басқару серверінен Kaspersky бағдарламалары үшін жаңартуларды алу	Дерекқор жаңартуларының көзі ретінде көрсетілген Басқару серверінен Kaspersky қолданбасының жаңартуларын алатын басқарылатын құрылғылар.
161	klnagent	SNMP	Желілік құрылғыларды бақылау және табу	Құрылғыларды табу.

klnagent процесі мақсатты құрылғының операциялық жүйесі порттарының динамикалық ауқымынан бос порттарды да сұрай алатынын ескеріңіз. Операциялық жүйе бұл порттарды klnagent процесіне автоматты түрде тағайындайды, сондықтан klnagent процесі басқа бағдарламалық жасақтама пайдаланатын кейбір порттарды пайдалануы мүмкін. Егер klnagent процесі осы бағдарламалық жасақтамаға әсер етсе, бағдарламалық жасақтамадағы порт параметрлерін өзгертіңіз немесе осы бағдарламалық жасақтама пайдаланатын портты қоспау үшін операциялық жүйеңіздегі әдепкі бойынша порттың динамикалық ауқымын өзгертіңіз.

Kaspersky Security Center қолданбасының үшінші тарап бағдарламалық құралымен үйлесімділігі туралы ұсыныстар тек анықтама үшін берілгенін және үшінші тарап бағдарламалық құралының жаңа нұсқаларына қолданылмауы мүмкін екенін ескеріңіз. Порттарды орнату бойынша сипатталған ұсыныстар техникалық қолдау қызметінің тәжірибесіне және ең жақсы тәжірибелерімізге негізделген.

Төмендегі кестеде тарату нүктесі рөлін атқаратын желілік агенті орнатылған басқарылатын құрылғыда қолданылатын порттар көрсетілген. Көрсетілген порттар желілік агенттер қолданатын порттарға қосымша ретінде тарату нүктесі құрылғыларында қолданылады (жоғарыдағы кестені қараңыз).

Тарату нүктесі ретінде жұмыс істейтін Желілік агент қолданатын порттар

Порт нөмірі	Портты ашатын процесс атауы	Протокол	Портты тағайындау	Аймақ
13000	klnagent	TCP (TLS)	Тарату нүктесі демилитаризацияланған аймақта қосылым шлюзі ретінде әрекет еткен кезде Желілік агенттерден және Kaspersky Security Center-ден қосылымдар қабылдау. Басқару сервері орнатылған құрылғы тарату нүктесі ретінде көрсетілсе, SSL қосылымы үшін әдепкі бойынша 13000 портының орнына 13001 порты пайдаланылады.	Клиент құрылғыларын басқару, жаңартулар мен орнату пакеттерін жеткізу. Толығырақ келесі бөлімді қараңыз: Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы. Әдепкі бойынша порт нөмірін Басқару консолінде тарату нүктесі сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
13111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	TCP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт нөмірін Басқару консолінде тарату нүктесі сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
15111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	UDP	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт нөмірін Басқару консолінде тарату нүктесі сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
17111 (құрылғыда KSN прокси-сервері қызметі іске қосылған болса ғана)	ksnproxy	HTTPS	Басқарылатын құрылғылардан KSN прокси-серверіне қатысты сұрауларды қабылдау	KSN прокси-сервері. Әдепкі бойынша порт нөмірін Басқару консолінде тарату нүктесі сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.
13295 (тарату нүктесін push-сервер ретінде қолдансаңыз ғана)	klnagent	TCP (TLS)	Клиент құрылғыларынан қосылымдар қабылдау	Push-сервер. Әдепкі бойынша порт нөмірін Басқару консолінде тарату нүктесі сипаттары терезесінде немесе Kaspersky Security Center Web Console веб-консолінде өзгерте аласыз.

Төмендегі кестеде домен контроллері құрылғысында пайдаланылатын порттар көрсетілген.

Домен контроллері құрылғысында пайдаланылатын порттар

Порт нөмірі	Протокол	Портты тағайындау	Аймақ
389	TCP немесе UDP арқылы LDAP	LDAP серверіне қосылу	Домен контроллері сауалнамасы
636	TLS арқылы LDAP	LDAP серверіне қосылу	Домен контроллері сауалнамасы

Төмендегі кестеде, Желілік агент орнатылмаған клиент құрылғыларында ашық болуы тиісті порт қамтылған.

Тағайындалмаған клиент құрылғысында пайдаланылатын порт

Порт нөмірі	Протокол	Портты тағайындау	Аймақ
22	SSH	SSH арқылы клиент құрылғысына қосылуда	Тек Linux негізіндегі клиент құрылғылары үшін. Linux тарату нүктесі арқылы Kaspersky қолданбаларын қашықтан орнату.

Kaspersky Security Center-мен жұмыс істеуге арналған сертификаттар

Бұл бөлімде Kaspersky Security Center сертификаттары туралы ақпарат бар және Басқару сервері үшін пайдаланушы сертификатын қалай шығару керектігін сипаттайды.

Kaspersky Security Center сертификаттары туралы

Kaspersky Security Center, бағдарламаның құрамдастары арасында қауіпсіз өзара әрекеттесуді қамтамасыз ету үшін келесі сертификат түрлерін пайдаланады:

- Басқару сервері сертификаты
- Ұялы құрылғы сертификаты
- iOS MDM сервері сертификаты
- Kaspersky Security Center Web Server сертификаты
- Kaspersky Security Center Web Console сертификаты

Әдепкісінше Kaspersky Security Center өздігінен қол қойылған сертификаттарды (яғни Kaspersky Security Center өзі шығарған) пайдаланады, бірақ ұйымыңыздың желісінің талаптарына жақсырақ жауап беру және қауіпсіздік стандарттарына сәйкес болу үшін оларды арнаулы сертификаттармен ауыстыруға болады. Басқару сервері пайдаланушы сертификатының барлық қолданыстағы талаптарға сәйкестігін тексергеннен кейін, бұл сертификат өздігінен қол қойылған сертификатпен бірдей әрекет ету ауқымына ие болады. Жалғыз айырмашылығы, пайдаланушы сертификаты жарамдылық мерзімі аяқталғаннан кейін автоматты түрде қайта шығарылмайды. Сіз сертификаттарды klsetsrvcert утилитасы арқылы немесе сертификат түріне байланысты Басқару сервері сипаттарындағы Басқару консолімен ауыстырасыз. klsetsrvcert утилитасын пайдалану кезінде келесі мәндердің бірін пайдаланып, сертификат түрін көрсету қажет:

- C – 13000 және 13291 порттары үшін жалпы сертификат.
- CR – 13000 және 13291 порттары үшін жалпы резервтік сертификат.
- M – 13292-порт үшін ұялы құрылғы сертификаты.
- MR – 13292-порт үшін резервтік ұялы құрылғы сертификаты.
- MCA – пайдаланушы сертификаттарын автоматты түрде жасау үшін сенімді сертификаттау орталығынан алынған мобильдік құрылғы сертификаты.

klsetsrvcert утилитасын жүктеудің қажеті жоқ. Утилита Kaspersky Security Center жеткізу жиынтығының құрамына кіреді. Утилита Kaspersky Security Center бағдарламасының алдыңғы нұсқаларымен үйлесімді емес.

Кез келген Басқару сервері сертификатының ең көп жарамдылық мерзімі 397 күннен аспауы керек.

Басқару серверінің сертификаттары

Басқару сервері сертификаты басқару серверінің түпнұсқалық растамасы үшін, сондай-ақ басқарылатын құрылғылардағы басқару сервері мен желілік агент және негізгі басқары сервері мен тәуелді серверлер арасында қауіпсіз өзара әрекеттесу үшін қажет. Басқару консолін Басқару серверіне алғаш қосқан кезде сізден ағымдағы Басқару сервері сертификатын пайдалануды растау сұралады. Мұндай растау, Басқару сервері сертификатын ауыстырған сайын, Басқару серверін әрбір рет қайта орнатқаннан кейін және қосалқы Басқару серверін негізгі Басқару серверіне қосқан кезде де қажет. Мұндай сертификат жалпы ("C") деп аталады.

Ортақ сертификат ("C") басқару серверінің құрамдасын орнатқан кезде автоматты түрде жасалады. Сертификат екі бөліктен тұрады:

- klserver.cer; файлы, ол әдепкі бойынша басқару серверінің құрамдасы орнатылған құрылғыда, C:\ProgramData\KasperskyLab\adminkit\1093\cert қалтасында орналасады.

- Құпия кілт Windows қорғалған қоймасында (Windows Protected Storage) болады.

Сондай-ақ, жалпы резервтік сертификат ("CR") бар. Kaspersky Security Center бағдарламасы бұл сертификатты жалпы сертификаттың мерзімі аяқталғанға дейін 90 күн бұрын автоматты түрде жасайды. Жалпы резервтік сертификат кейіннен Басқару сервері сертификатын ауыстыру үшін қолданылады. Жалпы сертификаттың мерзімі аяқталған кезде, басқарылатын құрылғыларда орнатылған Желілік агент үлгілерімен байланысты сақтау үшін жалпы резервтік сертификат қолданылады. Осы мақсатта жалпы резервтік сертификат ескі жалпы сертификаттың мерзімі аяқталғанға дейін 24 сағат бұрын автоматты түрде жаңа жалпы сертификатқа айналады.

Сондай-ақ, Басқару серверін деректерді жоғалтпай бір құрылғыдан екіншісіне тасымалдау үшін Басқару сервері сертификатының сақтық көшірмесін Басқару серверінің басқа параметрлерінен бөлек жасауға болады.

Ұялы құрылғы сертификаттары

Мобильді сертификаты ("M") ұялы құрылғылардағы Басқару серверінің түпнұсқалық растамасы үшін керек. Сіз ұялы құрылғы сертификатын пайдалануды бағдарламаны жылдам іске қосу шеберінің қадамында конфигурациялайсыз.

Сондай-ақ, резервтік ұялы құрылғы сертификаты ("MR") бар: ол ұялы құрылғы сертификатын ауыстыру үшін қолданылады. Kaspersky Security Center бағдарламасы бұл сертификатты жалпы сертификаттың мерзімі аяқталғанға дейін 60 күн бұрын автоматты түрде жасайды. Ұялы құрылғы сертификатының мерзімі аяқталған кезде, басқарылатын ұялы құрылғыларда орнатылған Желілік агентпен байланысты сақтау үшін резервтік ұялы құрылғы сертификаты қолданылады. Осы мақсатта резервтік ұялы құрылғы сертификаты ескі ұялы құрылғы сертификатының мерзімі аяқталғанға дейін 24 сағат бұрын автоматты түрде жаңа ұялы құрылғы сертификатына айналады.

Қосылу сценарийі мобильдік құрылғыларда клиент сертификатын пайдалануды талап етсе (екі жақты SSL түпнұсқалық растамасы арқылы қосылу), бұл сертификаттарды автоматты түрде жасалған пайдаланушы сертификаттары ("MCA") үшін сенімді сертификаттау орталығы арқылы жасайсыз. Сонымен қатарбастапқы орнату шебері басқа сенімді сертификаттау орталығы шығарған пайдаланушы сертификаттарын пайдалануды бастауға мүмкіндік береді, ал ұйымыңыздың жалпыға ортақ кілттер инфрақұрылымымен (PKI) біріктіру арқасында доменді сертификаттау орталығы арқылы клиент сертификаттарын шығаруға болады.

iOS MDM сервері сертификаты

iOS MDM сервер сертификаты iOS операциялық жүйесінің басқаруымен жұмыс істейтін ұялы құрылғылардағы Басқару серверінің түпнұсқалық растамасы үшін қажет. Бұл құрылғылармен өзара әрекеттесу, Желілік агентті пайдаланбайтын Apple Mobile Device Management (MDM) протоколы арқылы жүзеге асырылады. Оның орнына, сіз екі жақты SSL түпнұсқалық растамасын қамтамасыз ету үшін әр құрылғыға клиент сертификаты бар арнайы iOS MDM профилін орнатасыз.

Сонымен қатарбастапқы орнату шебері басқа сенімді сертификаттау орталығы шығарған пайдаланушы сертификаттарын пайдалануды бастауға мүмкіндік береді, ал ұйымыңыздың жалпыға ортақ кілттер инфрақұрылымымен (PKI) біріктіру арқасында доменді сертификаттау орталығы арқылы клиент сертификаттарын шығаруға болады.

Клиент сертификаттары iOS MDM профильдерін жүктеген кезде iOS құрылғыларына беріледі. iOS MDM серверінің пайдаланушы сертификаты әрбір iOS басқарылатын құрылғысы үшін бірегей. Автоматты түрде жасалған пайдаланушы сертификаттары ("MCA") үшін сенімді сертификаттау орталығы арқылы iOS MDM серверінің барлық клиент сертификаттарын жасайсыз.

Kaspersky Security Center Web Server сертификаты

Kaspersky Security Center веб-сервері (бұдан әрі — веб-сервер) Kaspersky Security Center басқару серверінің құрамдасы болып табылады және арнайы сертификат түрін пайдаланады. Бұл сертификат, сіз кейіннен басқарылатын құрылғыларға жүктейтін Желілік агенттің орнату пакеттерін жариялау үшін, сондай-ақ iOS MDM профильдерін, iOS қолданбаларын және Kaspersky Security for Mobile орнату пакеттерін жариялау үшін қажет. Ол үшін Веб-сервер әртүрлі сертификаттарды қолдана алады.

Егер ұялы құрылғыларды қолдау өшірулі болса, онда Веб-сервер келесі сертикаттардың бірін басымдық тәртібінде қолданады:

1. Басқару консолі арқылы қолмен көрсетілген Веб-сервердің пайдаланушы сертификаты.
2. Басқару серверінің жалпы сертификаты ("C").

Егер ұялы құрылғыларды қолдау қосулы болса, онда Веб-сервер келесі сертикаттардың бірін басымдық тәртібінде қолданады:

1. Басқару консолі арқылы қолмен көрсетілген Веб-сервердің пайдаланушы сертификаты.
2. Пайдаланушы ұялы құрылғы сертификаты.
3. Өздігінен қол қойылған ұялы құрылғы сертификаты ("M").
4. Басқару серверінің жалпы сертификаты ("C").

Kaspersky Security Center Web Console сертификаты

Kaspersky Security Center Web Console Server серверінің (бұдан әрі Web Console деп те аталады) өз сертификаты бар. Сіз сайтты ашқан кезде, браузер сіздің қосылымыңыздың сенімді ме екенін тексереді. Web Console сертификаты Web Console түпнұсқалық растамасын жасауға мүмкіндік береді және браузер мен Web Console арасындағы трафикті шифрлау үшін қолданылады.

Web Console ашқан кезде, браузер сізге Web Console қосылымы жеке емес екенін және Web Console сертификаты жарамсыз екенін хабарлауы мүмкін. Бұл ескерту, Kaspersky Security Center Web Console сертификаты өздігінен қол қоятындықтан және оны Kaspersky Security Center автоматты түрде жасайтындықтан пайда болады. Бұл ескертуді жою үшін келесі әрекеттердің бірін орындауға болады:

- Kaspersky Security Center Web Console сертификатын пайдаланушы сертификатына ауыстырыңыз (ұсынылатын параметр). Сіздің инфрақұрылымыңызда сенімді болып табылатын және пайдаланушы сертификаттарының талаптарына сәйкес келетін сертификат жасау.

- Web Console сертификатын браузердің сенімді сертификаттары тізіміне қосу. Бұл параметрді пайдаланушы сертификатын жасай алмаған жағдайда ғана пайдалану ұсынылады.

Басқару серверінің сертификаты туралы

Басқару серверінің сертификатын пайдалану арқылы екі операция орындалады: Басқару консолі қосылған кезде Басқару серверінің түпнұсқалық растамасы және құрылғылармен деректер алмасу. Сертификат негізгі Басқару серверлері қосалқы Басқару серверлеріне қосылған кезде түпнұсқалық растама үшін де қолданылады.

Kaspersky берген сертификаттар

Басқару серверінің сертификаты, Басқару сервері құрамдасын орнату кезінде автоматты түрде жасалады және %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert қалтасында сақталады.

Басқару серверінің сертификаты, егер сертификат 12.2 немесе одан бұрынғы нұсқадағы Басқару сервері арқылы жасалған болса, бес жылға жарамды болады. Әйтпесе, сертификаттың жарамдылық мерзімі 397 күнмен шектеледі. Басқару сервері жаңа сертификатты резервтік сертификат ретінде, ағымдағы сертификаттың әрекетінің аяқталу мерзімінен 90 күн бұрын жасайды. Содан кейін, жарамдылық мерзімі аяқталғанға дейін бір күн бұрын жаңа сертификат ағымдағы сертификатты автоматты түрде ауыстырады. Клиент құрылғыларындағы барлық Желілік агенттер жаңа сертификатты пайдалану арқылы Басқару серверімен автоматты түрде түпнұсқалық растамаға конфигурацияланады.

Пайдаланушы сертификаттары

Қажет болса, Басқару сервері сертификатына пайдаланушы сертификатын тағайындауға болады. Мысалы, бұл сіздің ұйымыңыздың бұрыннан бар PKI жүйесімен жақсырақ интеграциялау үшін немесе сертификат өрістерінің қажетті конфигурациясы үшін қажет болып қалуы мүмкін.

Кез келген Басқару сервері сертификатының ең көп жарамдылық мерзімі 397 күннен аспауы керек.

Сертификатты ауыстырған кезде, бұрын SSL арқылы Басқару серверіне қосылған барлық Желілік агенттер Серверге "Басқару серверінің түпнұсқалық растамасы қатесі" қатесімен қосылуды тоқтатады. Бұл қатені жою үшін, сізге сертификатты ауыстырғаннан кейін қосылымды қалпына келтіру керек.

Басқару серверінің сертификаты жоғалған болса, оны қалпына келтіру үшін Басқару сервері құрамдасын қайта орнату және деректерді қалпына келтіру керек болады.

Егер сіз әртүрлі браузерлерде Kaspersky Security Center Web Console бағдарламасын ашып, Басқару сервері сипаттары терезесінде Басқару сервері сертификатының файлын жүктесеңіз, жүктелген файлдардың атаулары әртүрлі болады.

Kaspersky Security Center-де қолданылатын пайдаланушы сертификаттарына қойылатын талаптар

Төмендегі кестеде, Kaspersky Security Center түрлі құрамдастарына қатысты пайдаланушы сертификаттарына қойылатын талаптар көрсетілген.

Kaspersky Security Center сертификаттарына қойылатын талаптар

Сертификат түрі	Талаптар	Түсіндірмелер
Жалпы сертификат, жалпы резервтік сертификат ("C", "CR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • Жол ұзындығын шектеу: Жоқ. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кілтті кеңейтілген пайдалану (Extended Key Usage, EKU) (міндетті емес): Сервердің түпнұсқалық растамасы, клиенттің түпнұсқалық растамасы. Сертификатта Басқару серверінің кері байланыс мекенжайын қамтитын жарамды Субъектінің баламалы атауы (SAN) болуы керек: • IPv4 үшін: 127.0.0.1 • IPv6 үшін: 0:0:0:0:0:0:0:1	Extended Key Usage параметрі міндетті емес. Жолдың ұзындығын шектеу мәндері "None" мәнінен ерекшеленетін бүтін сан болуы мүмкін, бірақ 1-ден кем болмауы тиіс.

Сертификат түрі	Талаптар	Түсіндірмелер
Ұялы құрылғы сертификаты, резервтік ұялы құрылғы сертификаты ("M", "MR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (EKU) (міндетті емес): Сервердің түпнұсқалық растамасы.	Extended Key Usage параметрі міндетті емес. Егер жалпы сертификатта жол ұзындығын шектеу мәні кемінде 1 болса, жол ұзындығын шектеу мәні "None" мәнінен басқа бүтін сан болуы мүмкін.
Автоматты түрде жасалатын пайдаланушы сертификаттары (MCA) үшін сенімді сертификаттау орталығы (CA) шығарған сертификат	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кілтті кеңейтілген пайдалану (Extended Key Usage, EKU) (міндетті емес): Сервердің түпнұсқалық растамасы, клиенттің түпнұсқалық растамасы.	Extended Key Usage параметрі міндетті емес. Егер жалпы сертификатта жол ұзындығын шектеу мәні кемінде 1 болса, жол ұзындығын шектеу мәні "None" мәнінен басқа бүтін сан болуы мүмкін.
Веб-сервер сертификаты	Кеңейтілген кілт қолданысы (EKU): Сервердің түпнұсқалық растамасы. Сертификаты көрсетілетін PKCS #12 / PEM контейнері жалпыға ортақ кілттердің барлық тізбегін қамтиды. Субъектінің баламалы атауы (SAN) бар; яғни `subjectAltName` өрісі толтырылған. Сертификат серверлер сертификаттарына қойылатын браузерлердің қолданыстағы талаптарына, сондай-ақ CA/Browser Forum ағымдағы базалық талаптарына сай келеді.	—
Kaspersky Security Center Web Console сертификаты	Сертификаты көрсетілетін PEM контейнері жалпыға ортақ кілттердің барлық тізбегін қамтиды. Субъектінің баламалы атауы (SAN) бар; яғни `subjectAltName` өрісі толтырылған. Сертификат серверлер сертификаттарына қойылатын браузерлердің қолданыстағы талаптарына, сондай-ақ CA/Browser Forum ағымдағы базалық талаптарына сай келеді.	Шифрланған сертификаттарға Kaspersky Security Center Web Console қолдау көрсетпейді.

Сценарий: Басқару серверінің пайдаланушы сертификатын белгілеу

Сіз өзіңіздің ұйымыңыздың қолданыстағы жалпыға ортақ кілттер инфрақұрылымымен (PKI) жақсырақ біріктіру үшін немесе сертификат параметрлерінің пайдаланушы конфигурациясы үшін Басқару серверінің пайдаланушы сертификатын тағайындай аласыз. Сертификатты, Басқару серверін орнатқаннан кейін, бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғанға дейін ауыстырған жөн.

Кез келген Басқару сервері сертификатының ең көп жарамдылық мерзімі 397 күннен аспауы керек.

Алдын ала талаптар

Келесі шарттар орындалуы керек:

- Сертификат PKCS#12 пішімінде жасалуы керек (мысалы, ұйымның PKI арқылы).
- Жаңа сертификат үшін төмендегі кестеде көрсетілген талаптар орындалуы керек.

  Төмендегі кестеде "CA: true" талабына назар аударыңыз, бұл жаңа сертификатты сенімді сертификаттау орталығы (CA) беруі керек дегенді білдіреді. "CA: true" талабы бар жаңа сертификат бүкіл сенім тізбегін және pfx немесе p12 кеңейтімі бар файлда сақталуы тиісті жеке кілтті қамтуы керек.

Басқару серверінің сертификаттарына қойылатын талаптар

Сертификат түрі	Талаптар
Жалпы сертификат, жалпы резервтік сертификат ("C", "CR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • Жол ұзындығын шектеу: Жоқ. Жол ұзындығын шектеу мәні "None" мәнінен басқа, бірақ 1-ден кем емес бүтін сан болуы мүмкін. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (Extended Key Usage, EKU) (міндетті емес): Сервердің түпнұсқалық растамасы және клиенттің түпнұсқалық растамасы. EKU міндетті емес, бірақ ол сіздің сертификатыңызда болса, Сервер мен клиенттің түпнұсқалық растамасы деректері EKU-да көрсетілуі керек. Сертификатта жарамды Субъектінің баламалы атауы (SAN) болуы керек. `subjectAltName` өрісінде Басқару серверінің кері байланыс мекенжайы болуы керек: • IPv4 үшін: 127.0.0.1 • IPv6 үшін: 0:0:0:0:0:0:0:1
Ұялы құрылғы сертификаты, резервтік ұялы құрылғы сертификаты ("M", "MR")	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Егер жалпы сертификатта жол ұзындығын шектеу мәні кемінде 1 болса, жол ұзындығын шектеу мәні "None" мәнінен басқа бүтін сан болуы мүмкін. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (EKU): Сервердің түпнұсқалық растамасы. EKU міндетті емес, бірақ ол сіздің сертификатыңызда болса, Сервердің түпнұсқалық растамасы деректері EKU-да көрсетілуі керек.

Сертификат түрі	Талаптар
Автоматты түрде жасалатын пайдаланушы сертификаттары (MCA) үшін сенімді сертификаттау орталығы (CA) шығарған сертификат	Кілттің минималды ұзындығы: 2048. Негізгі шектеулер: • CA: Иә. • Жол ұзындығын шектеу: Жоқ. Егер жалпы сертификатта жол ұзындығын шектеу мәні кемінде 1 болса, жол ұзындығын шектеу мәні "None" мәнінен басқа бүтін сан болуы мүмкін. Кілтті пайдалану: • Сандық қолтаңба. • Сертификат қолтаңбасы. • Кілттерді шифрлау. • Кері қайтару тізіміне (CRL) қол қою. Кеңейтілген кілт қолданысы (EKU): клиент аутентификациясы. EKU міндетті емес, бірақ ол сіздің сертификатыңызда болса, клиенттің түпнұсқалық растамасы деректері EKU-да көрсетілуі керек.

Сенімді сертификаттау орталығы (ағылшынша certificate authority, CA) шығарған сертификаттардың сертификаттарға қол қоюға рұқсаты жоқ. Мұндай сертификаттарды пайдалану үшін, желіңіздегі тарату нүктелерінде немесе қосылым шлюздерінде 13 немесе одан жоғары нұсқадағы Желілік агент орнатылғанына көз жеткізіңіз. Әйтпесе, сіз қол қою рұқсатынсыз сертификаттарды пайдалана алмайсыз.

Кезеңдер

Басқару сервері сертификатын көрсету келесі кезеңдерден тұрады:

1. **Басқару серверінің сертификатын ауыстыру**

   Осы мақсат үшін klsetsrvcert пәрмен жолы утилитасын пайдаланыңыз.

2. **Жаңа сертификатты көрсету және Желілік агенттердің Басқару серверімен байланысын қалпына келтіру**

   Сертификатты ауыстырған кезде, бұрын SSL арқылы Басқару серверіне қосылған барлық Желілік агенттер Серверге "Басқару серверінің түпнұсқалық растамасы қатесі" қатесімен қосылуды тоқтатады. Жаңа сертификатты көрсету және қосылымды қалпына келтіру үшін klmover утилитасының пәрмен жолын пайдаланыңыз.

3. **Kaspersky Security Center Web Console параметрлерінде жаңа сертификатты көрсету**

   Сертификатты ауыстырғаннан кейін, мұны Kaspersky Security Center Web Console параметрлерінде көрсетіңіз. Әйтпесе, Kaspersky Security Center Web Console Басқару серверіне қосыла алмайды.

Нәтижелер

Сценарий аяқталғаннан кейін, Басқару сервері сертификаты ауыстырылады, басқарылатын құрылғылардағы Желілік агент сервері жаңа сертификатты пайдалану арқылы Серверді аутентификациялайды.

klsetsrvcert утилитасын пайдаланып, Басқару сервері сертификатын ауыстыру

Басқару сервері сертификатын ауыстыру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
klsetsrvcert [-t <сертификат түрі> {-i <жаңа сертификатқа жол> [-p <құпиясөз>] [-o <параметрлер>] | -g <dns атауы>}][-f <ауыстыру уақыты>][-r <түбірлік сертификаттар>][-l <журнал файлының жолы>]
```

klsetsrvcert утилитасын жүктеудің қажеті жоқ. Утилита Kaspersky Security Center жеткізу жиынтығының құрамына кіреді. Ол Kaspersky Security Center алдыңғы нұсқаларымен үйлеспейді.

klsetsrvcert утилитасының параметрлерінің сипаттамасы төмендегі кестеде келтірілген.

klsetsrvcert утилитасының параметрлерінің мәндері

Параметр	Мән
`-t < сертификат түрі >`	Ауыстырылатын сертификат түрі. `< сертификат түрі >` параметрінің ықтимал мәндері: • `C` – 13000 және 13291 порттары үшін жалпы сертификатты ауыстыру. • `CR` – 13000 және 13291 порттары үшін жалпы резервтік сертификатты ауыстыру. • `M` – 13292 портының ұялы құрылғыларына арналған сертификатты ауыстырыңыз. • `MR` – 13292-порт үшін резервтік ұялы құрылғы сертификатын ауыстыру. • `MCA` – пайдаланушы сертификаттарын автоматты түрде жасау үшін сенімді сертификаттау орталығынан алынған мобильдік құрылғы сертификаты.
`-f < ауыстыру уақыты >`	Сертификатты ауыстыру кестесі "КК-АА-ЖЖЖЖ СС:ММ" пішімін қолданады (13000 және 13291 порттары үшін). Жалпы сертификат мерзімі аяқталмай тұрып, оны жалпы резервтік сертификатпен ауыстырғыңыз келсе, осы параметрді қолданыңыз. Басқарылатын құрылғылардың жаңа сертификатты пайдаланып Басқару серверімен синхрондау уақытын көрсетіңіз.
`-i < жаңа сертификатқа жол >`	Сертификаты бар контейнер және PKCS#12 пішіміндегі жеке кілт (p12 немесе pfx кеңейтімі бар файл).
`-p < құпиясөз >`	p12 контейнерін қорғайтын құпиясөз. Сертификат пен жеке кілт контейнерде сақталады, сондықтан контейнер файлын шифрсыздау үшін құпиясөз қажет.
`-o < тексеру параметрлері >`	Сертификатты тексеру параметрлері (нүктелі үтірмен бөлінген). Қол қоюға рұқсатсыз пайдаланушы сертификатын пайдалану үшін klsetsrvcert утилитасында `-o NoCA` көрсетіңіз. Бұл сенімді сертификаттау орталығы шығарған сертификаттар үшін пайдалы (ағылшынша certificate authority, CA). C немесе CR түріндегі сертификаттар үшін шифрлау кілтінің ұзындығын өзгерту үшін klsetsrvcert утилитасында `-o RsaKeyLen:< кілт ұзындығы >` деп көрсетіңіз, мұндағы `< кілт ұзындығы >` параметрі – қажетті кілт ұзындығы. Әйтпесе, ағымдағы сертификат кілтінің ұзындығы пайдаланылады.
`-g < dns атауы >`	Сертификат көрсетілген DNS атауымен жасалады.
`-r < түбірлік сертификаттар >`	Сенімді сертификаттау орталығы қол қойған PEM пішіміндегі сенімді түбірлік сертификаттардың тізімі.
`-l < журнал файлының жолы >`	Нәтижелерді шығару файлы. Әдепкі бойынша, шығару стандартты шығару ағынында жүзеге асырылады.

Мысалы, Басқару серверінің пайдаланушы сертификатын көрсету үшін келесі пәрменді пайдаланыңыз:

```
klsetsrvcert -t C -i <жаңа сертификатқа жол> -p <құпиясөз> -o NoCA
```

Сертификатты ауыстырғаннан кейін, SSL протоколы арқылы Басқару серверіне қосылған барлық Желілік агенттер байланысын жоғалтады. Байланысты қалпына келтіру үшін, klmover утилитасы пәрмен жолағын қолданыңыз.

Желілік агенттердің қосылымдарын жоғалтпау үшін келесі пәрмендерді пайдаланыңыз:

1. Жаңа сертификатты орнату үшін,

```
klsetsrvcert.exe -t CR -i <жаңа сертификатқа жол> -p <құпиясөз> -o NoCA
```

2. Жаңа сертификатқа өтінім беру күнін көрсету үшін,

```
klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
```

мұндағы "DD-MM-YYYY hh:mm" күні ағымдағы күннен 3-4 аптаға көбірек. Сертификатты жаңа сертификатқа ауыстыру уақытын ауыстыру жаңа сертификатты барлық Желілік агенттерге таратуға мүмкіндік береді.

Желілік агенттерді klmover утилитасын пайдаланып Басқару серверіне қосу

Басқару сервері сертификатын klsetsrvcert пәрмен жолының утилитасымен ауыстырғаннан кейін, байланыс үзілгендіктен Желілік агенттер мен Басқару сервері арасында SSL қосылымын орнату керек.

Жаңа Басқару сервер сертификатын көрсету және қосылымды қалпына келтіру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
klmover [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL портының нөмірі>]
[-nossl] [-cert <сертификат файлына апаратын жол>]
```

Утилитаны іске қосу үшін әкімші құқықтары қажет.

Бұл утилита Желілік агентті клиент құрылғысына орнатқан кезде Желілік агенттің орнату қалтасына автоматты түрде көшіріледі.

Зиянкестер құрылғыларды Басқару серверіңіздің басқаруынан шығаруына жол бермеу үшін klmover утилитасын іске қосқан кезде құпия сөзбен қорғауды міндетті түрде қосу ұсынылады. Құпиясөз қорғанысын қосу үшін Желілік агент саясаты параметрлерінде **Жою құпиясөзін пайдалану** опциясын таңдаңыз.

klmover утилитасына жергілікті әкімші құқықтары қажет. klmover утилитасын іске қосу үшін құпия сөзді қорғауды жергілікті әкімші құқықтарынсыз жұмыс істейтін құрылғылар үшін орнатпауға болады.

Жою құпиясөзін пайдалану параметрін қосу кезінде Cleaner (cleaner.exe) көмегімен құпиясөзді қорғау да қосылады.

Қосылым шлюздері арқылы басқару серверіне қосылған клиент құрылғылары үшін klmover утилитасын пайдалана алмайсыз. Мұндай құрылғылар үшін Желілік агентті қайта конфигурациялау немесе желілік агентті қайта орнату және қосылым шлюзін көрсету керек.

klmover утилитасының параметрлерінің сипаттамасы төмендегі кестеде келтірілген.

klmover утилитасының параметрлерінің мәндері

Параметр	Мән
`-address < сервер мекенжайы >`	Қосылу үшін Басқару сервері мекенжайы. Мекенжай ретінде IP мекенжайын, NetBIOS- немесе DNS атауын көрсетуге болады.
`-pn < порт нөмірі >`	Басқару серверіне шифрланбаған қосылу орындалатын порт нөмірі. Әдепкі бойынша 14000-порт орнатылған.
`-ps < SSL порты нөмірі >`	SSL протоколын қолдана отырып, Басқару серверіне шифрланған қосылу жүзеге асырылатын SSL порты нөмірі. Әдепкі бойынша 13000-порт орнатылған.
`-nossl`	Басқару серверіне шифрланбаған қосылымды пайдалану. Егер кілт пайдаланылмаса, Желілік агент Серверге қорғалған SSL протоколы арқылы қосылады.
`-cert < сертификат файлының жолы >`	Басқару серверіне қатынасудың түпнұсқалық растамасын жасау үшін көрсетілген сертификат файлын пайдалану.
`-virtserv`	Виртуалды Басқару серверінің атауы.
`-cloningmode`	Желілік агенттің дискісін клондау режимі. Дискіні клондау режимін конфигурациялау үшін келесі параметрлердің бірін пайдаланыңыз: • `-cloningmode` – дискіні клондау режимінің күйін сұрау. • `-cloningmode 1` – дискіні клондау режимін қосу. • `-cloningmode 0` – дискіні клондау режимін өшіру.
`-nauninstpwd < құпиясөз >`	Бұл параметрді желілік агенттің жою құпиясөзін көрсету үшін пайдаланыңыз. Параметр міндетті емес.

Мысалы, Желілік агентті Басқару серверіне қосу үшін келесі пәрменді орындаңыз:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Веб-сервер сертификатын қайта шығару

Kaspersky Security Center бағдарламасында қолданылатын Веб-сервер сертификаты, сіз кейіннен басқарылатын құрылғыларға жүктейтін Желілік агенттің орнату пакеттерін жариялау үшін, сондай-ақ iOS MDM профильдерін, iOS қолданбаларын және Kaspersky Endpoint Security for Mobile орнату пакеттерін жариялау үшін қажет. Ағымдағы қолданба конфигурациясына байланысты әртүрлі сертификаттар веб-сервер сертификаты ретінде жұмыс істейді (қосымша ақпаратты Kaspersky Security Center сертификаттары туралы ақпарат бөлімінен қараңыз).

Қолданбаны жаңартуды бастамай тұрып, ұйымыңыздың қауіпсіздік талаптарына сай болуын қамтамасыз ету немесе басқарылатын құрылғыларыңыздың тұрақты қосылымын қолдау үшін веб-сервер сертификатын қайта шығару қажет болуы мүмкін. Kaspersky Security Center веб-сервер сертификатын қайта шығарудың екі жолын ұсынады; екі әдіс арасындағы таңдау мобильдік құрылғылардың қосылғанына және мобильдік протокол арқылы басқарылатынына байланысты (яғни мобильдік сертификатты пайдалану арқылы).

Егер сіз ешқашан Басқару сервері сипаттарының **Веб-сервер** терезесінде Веб-сервер сертификаты ретінде пайдаланушы сертификатын көрсетпеген болсаңыз, ұялы құрылғы сертификаты Веб-сервер сертификаты ретінде қолданылады. Бұл жағдайда, Веб-сервер сертификатын қайта шығару мобильді протоколдың өзін қайта шығару арқылы жүзеге асырылады.

Мобильді протокол арқылы басқарылатын ұялы құрылғылар болмаған кезде Веб-сервер сертификатын қайта шығару үшін:

1. Консоль ағашында қажетті Басқару серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
2. Ашылған Басқару сервері сипаттары терезесінде **Басқару серверіне қосылу параметрлері** бөлімін таңдаңыз.
3. Бөлікшелер тізімінен **Сертификаттар** бөлікшесін таңдаңыз.
4. Егер сіз Kaspersky Security Center берген сертификатты одан әрі пайдалануды жоспарласаңыз:

   a. **Ұялы құрылғылармен Басқару серверін аутентификациялау** параметрлер тобынан **Сертификат Басқару серверінің құралдары арқылы шығарылған** параметрін таңдап, **Қайта шығару** түймесін басыңыз.

   b. Ашылған **Сертификатты қайта шығару** терезесінде, **Байланыстың мекенжайы** және **Белсендіру мерзімі** параметрлер тобында тиісті параметрлерді таңдап, **ОК** түймесін басыңыз.

   c. Пайда болған терезеде **Иә** түймесін басыңыз.

   Егер сіз өзіңіздің сертификатыңызды пайдалануды жоспарласаңыз, келесі әрекеттерді орындаңыз:

   a. Сіздің арнайы сертификатыңыз Kaspersky Security Center талаптарына сәйкес келетінін тексеріңіз. Қажет болса, сертификатты өзгертіңіз.

   b. **Басқа сертификат** параметрін таңдап, **Шолу** түймесін басыңыз.

   c. Ашылған **Сертификат** терезесінде, **Сертификат түрі** өрісінде өз сертификатыңыздың түрін таңдап, сертификаттың орналасуы мен параметрлерді көрсетіңіз:

      - **PKCS #12 контейнері** таңдасаңыз, **Сертификат файлы** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі сертификат файлын көрсетіңіз. Сертификат файлы құпиясөзбен қорғалған болса, **Құпиясөз (бар болса)** өрісінде құпиясөзді енгізіңіз.

      - **X.509 сертификаты** таңдасаңыз, **Жабық кілт (.prk, .pem)** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі жеке кілтті көрсетіңіз. Жеке кілт құпиясөзбен қорғалған болса, **Құпиясөз (бар болса)** өрісінде құпиясөзді енгізіңіз. **Жалпыға ортақ кілт (.cer)** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі жеке кілтті көрсетіңіз.

   d. **Сертификат** терезесінде **ОК** түймесін басыңыз.

   e. Пайда болған терезеде **Иә** түймесін басыңыз.

   Ұялы құрылғы сертификаты Веб-сервер сертификаты ретінде пайдалану үшін қайта шығарылды.

Мобильді протокол арқылы басқарылатын ұялы құрылғылар болған кезде Веб-сервер сертификатын қайта шығару үшін:

1. Пайдаланушы сертификатын жасаңыз және оны Kaspersky Security Center-де пайдалануға дайындаңыз. Сіздің арнайы сертификатыңыз Kaspersky Security Center талаптарына сәйкес келетінін тексеріңіз. Қажет болса, сертификатты өзгертіңіз.
2. Консоль ағашында қажетті Басқару серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
3. Ашылған Басқару сервері сипаттары терезесінде **Веб-сервер** бөлімін таңдаңыз.

4. **HTTPS протоколы бойынша** мәзірінде **Басқа сертификатты белгілеу** параметрін таңдаңыз.

5. **HTTPS протоколы бойынша** мәзірінде **Өзгерту** түймесін басыңыз.

6. Ашылған **Сертификат** терезесінде, **Сертификат түрі** өрісінде сертификатыңыздың түрін таңдаңыз:

   - **PKCS #12 контейнері** таңдасаңыз, **Сертификат файлы** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі сертификат файлын көрсетіңіз. Сертификат файлы құпиясөзбен қорғалған болса, **Құпиясөз (бар болса)** өрісінде құпиясөзді енгізіңіз.

   - **X.509 сертификаты** таңдасаңыз, **Жабық кілт (.prk, .pem)** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі жеке кілтті көрсетіңіз. Жеке кілт құпиясөзбен қорғалған болса, **Құпиясөз (бар болса)** өрісінде құпиясөзді енгізіңіз. **Жалпыға ортақ кілт (.cer)** өрісінің жанындағы **Шолу** түймесін басыңыз және қатты дискідегі жеке кілтті көрсетіңіз.

7. **Сертификат** терезесінде **OK** түймесін басыңыз.

8. Қажет болса, Басқару сервері сипаттары терезесінде, **Веб-сервердің HTTPS порты** өрісінде Веб-сервер үшін HTTPS портының нөмірін өзгертіңіз. **OK** түймесін басыңыз.

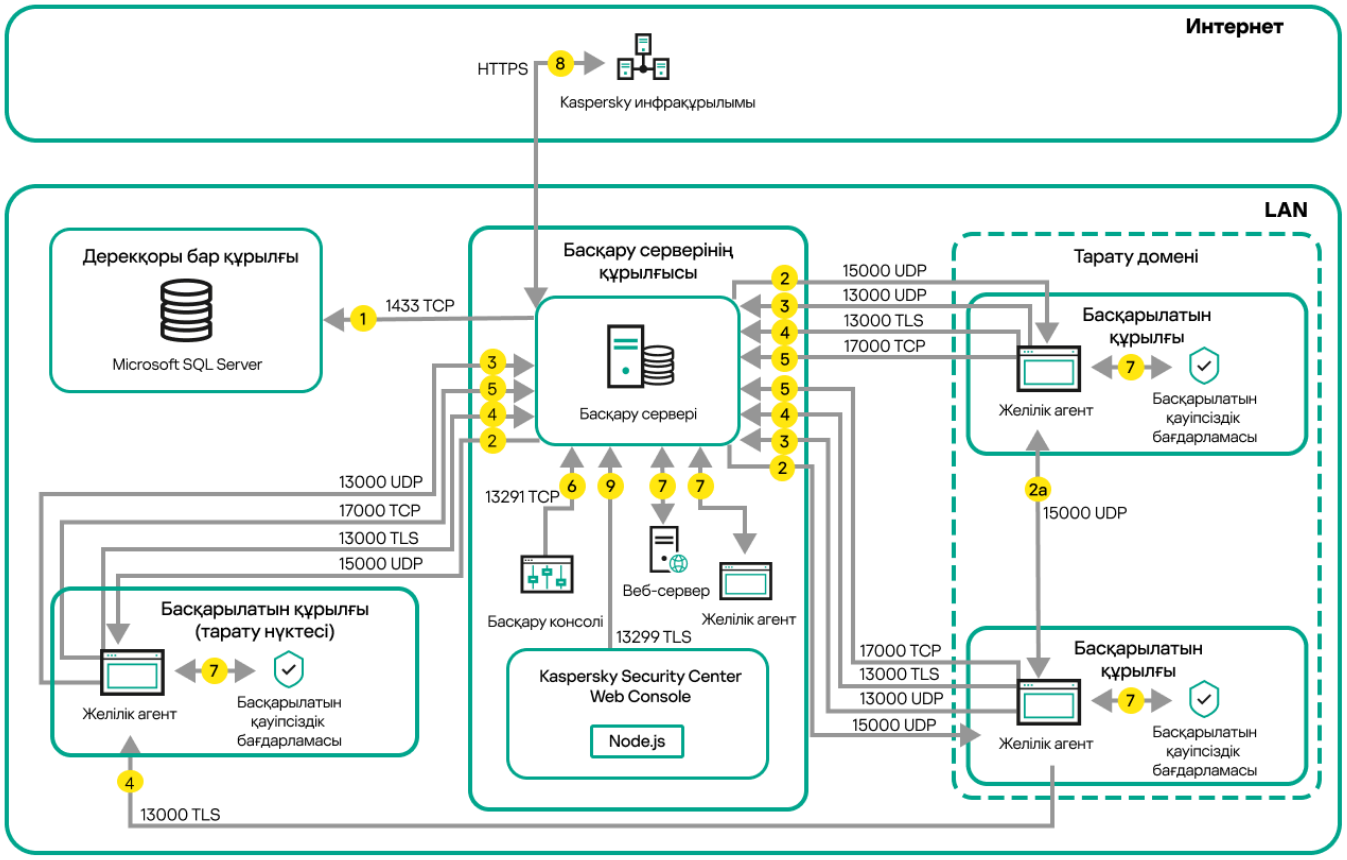
   Веб-сервер сертификаты қайта шығарылды.

Деректер трафигі және порттарды пайдалану схемалары

Бұл бөлімде Kaspersky Security Center құрамдастары, басқарылатын қауіпсіздік бағдарламалары және әртүрлі конфигурацияларға арналған сыртқы серверлер арасындағы деректер трафигінің схемалары берілген. Схемаларда жергілікті құрылғыларда қолжетімді болуы тиісті порт нөмірлері бар.

Жергілікті желідегі (LAN) Басқару сервері және басқарылатын құрылғылар

Төмендегі суретте, Kaspersky Security Center бағдарламасы тек жергілікті желіде (LAN) орналастырылған болса, деректер трафигі көрсетілген.



Жергілікті желідегі (LAN) Басқару сервері және басқарылатын құрылғылар

Суретте әртүрлі басқарылатын құрылғылардың Басқару серверіне әртүрлі тәсілдермен қалай қосылатыны көрсетілген: тікелей немесе тарату нүктесі арқылы. Тарату нүктелері, жаңартуларды тарату кезінде және желідегі трафикті оңтайландыру кезінде Басқару серверіне түсетін жүктемені азайтады. Алайда, тарату нүктелері, басқарылатын құрылғылардың саны айтарлықтай көп болған кезде ғана керек. Басқарылатын құрылғылардың саны аз болса, барлық басқарылатын құрылғылар жаңартуларды тікелей Басқару серверінен ала алады.

Нұсқарлар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт немесе Microsoft SQL Server үшін 1433-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

   > Kaspersky Security Center бағдарламасының ерте нұсқаларында тарату нүктесі жаңарту агенті деп аталған.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. MMC негізіндегі басқару консолі деректері 13291 порты арқылы басқару серверіне тасымалданады. (Басқару консолін бір немесе басқа құрылғыға орнатуға болады.)

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

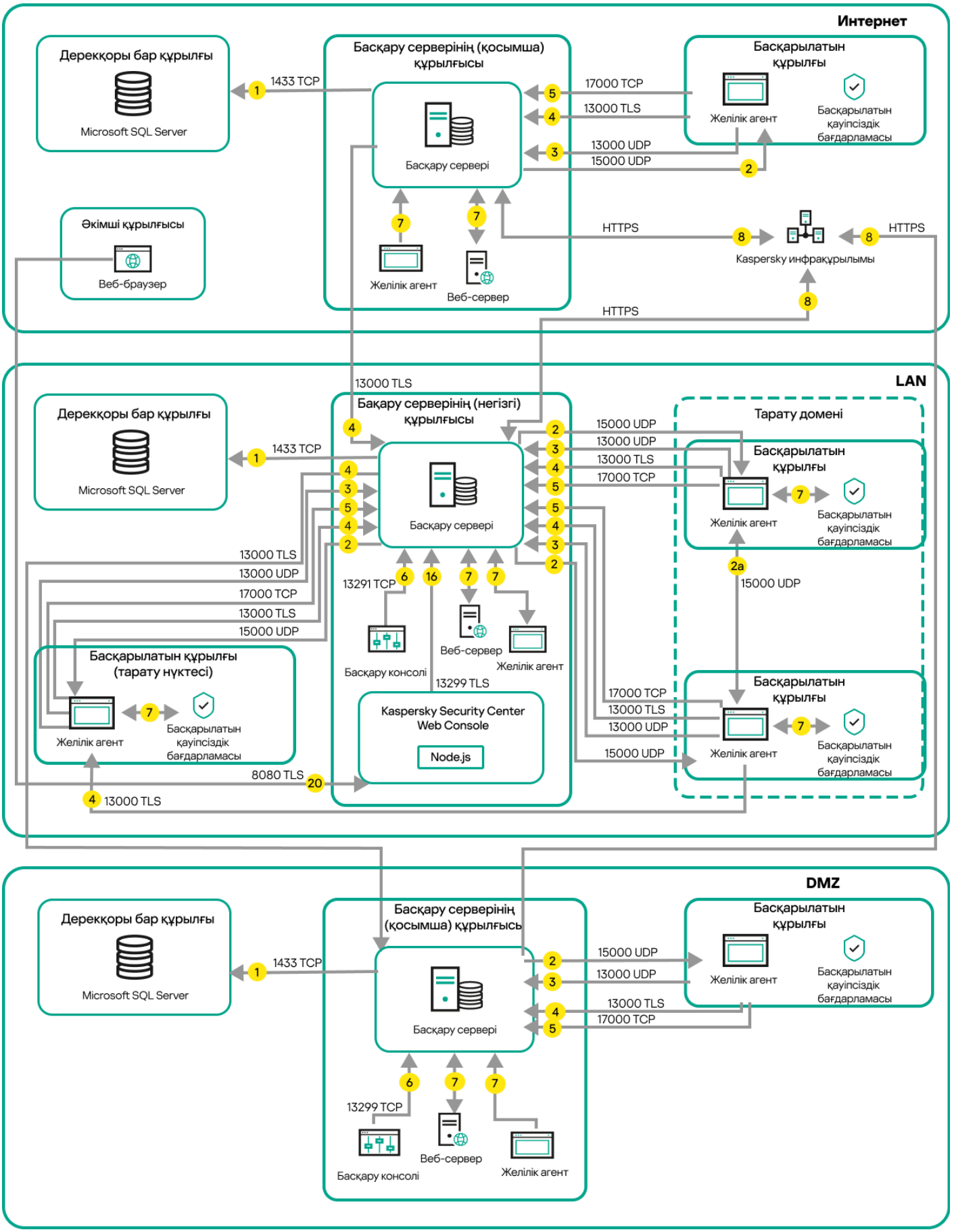
8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

Жергілікті желідегі (LAN) негізгі Басқару сервері және екі қосалқы Басқару сервері

Суретте Басқару серверлерінің иерархиясы көрсетілген: негізгі Басқару сервері жергілікті желіде (LAN) орналасқан. Қосалқы Басқару сервері демилитаризацияланған аймақта (DMZ) орналасқан; басқа қосалқы Басқару сервері интернетте орналасқан.



Басқару серверлерінің иерархиясы: негізгі Басқару сервері және екі қосалқы Басқару сервері

Нұсқарлар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт немесе Microsoft SQL Server үшін 1433-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

   > Kaspersky Security Center бағдарламасының ерте нұсқаларында тарату нүктесі жаңарту агенті деп аталған.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. MMC негізіндегі басқару консолі деректері 13291 порты арқылы басқару серверіне тасымалданады. (Басқару консолін бір немесе басқа құрылғыға орнатуға болады.)

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

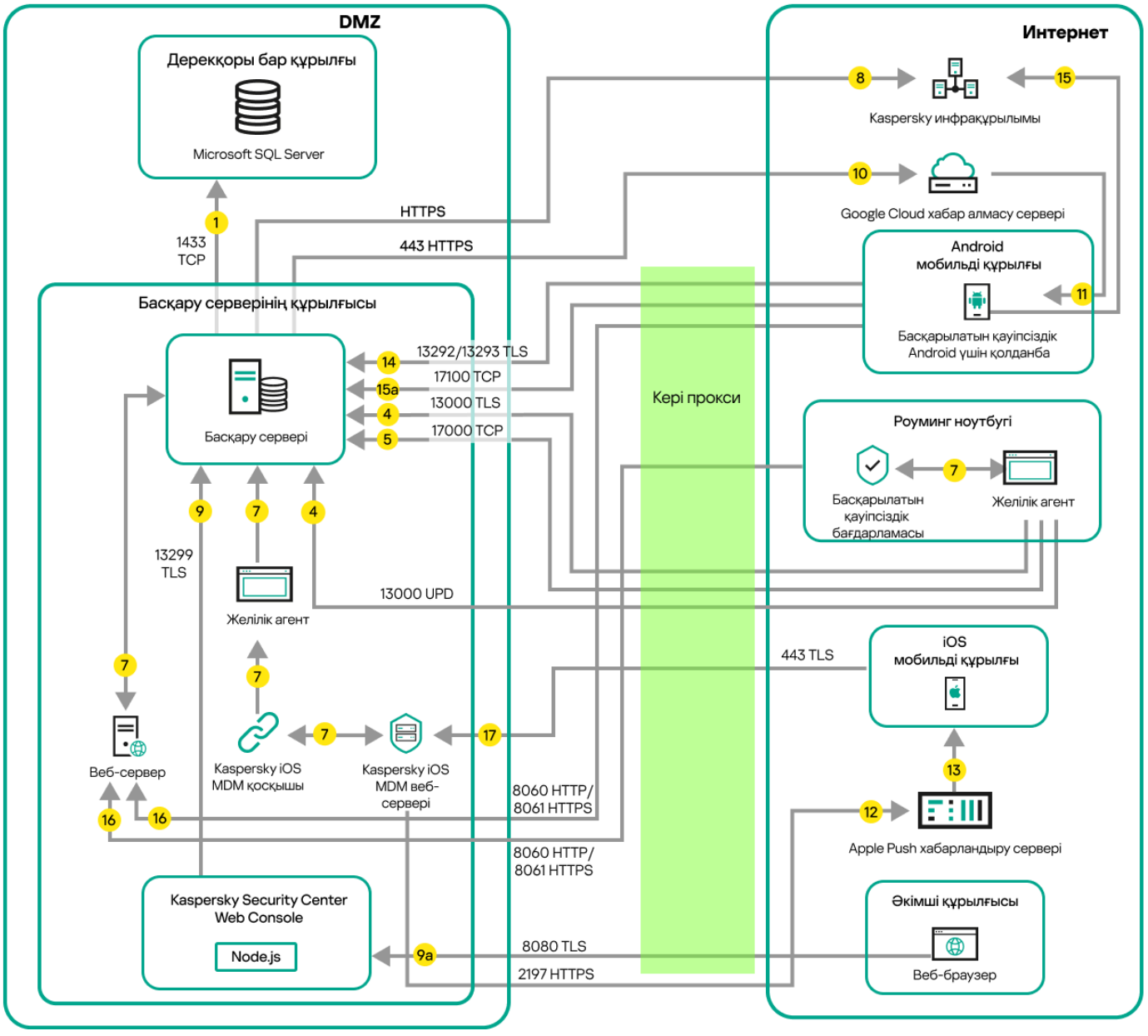
   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   9a. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

Жергілікті желі (LAN) ішіндегі басқару сервері, интернеттегі басқарылатын құрылғылар; кері прокси-серверді пайдалану

Төмендегі суретте, Басқару сервері жергілікті желі (LAN) ішінде, ал басқарылатын құрылғылар, сонымен қатар ұялы құрылғылар интернетте болатын деректер трафигі көрсетілген. Төмендегі сурет сіз таңдаған кері прокси-серверді пайдаланады. Қосымша ақпарат алу үшін осы бағдарламаның құжаттамасын қараңыз.



Жергілікті желідегі басқару сервері; басқарылатын құрылғылар басқару серверіне кері прокси-сервер арқылы қосылады

Бұл орналастыру схемасы, ұялы құрылғылар тікелей Басқару серверіне қосылғанын қаламасаңыз және қосылым шлюзін демилитаризацияланған аймақта (DMZ) тағайындауды қаламасаңыз, ұсынылады.

Нұсқарлар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт немесе Microsoft SQL Server үшін 1433-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

   > Kaspersky Security Center бағдарламасының ерте нұсқаларында тарату нүктесі жаңарту агенті деп аталған.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. MMC негізіндегі басқару консолі деректері 13291 порты арқылы басқару серверіне тасымалданады. (Басқару консолін бір немесе басқа құрылғыға орнатуға болады.)

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   9a. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

10. Тек Android ұялы құрылғылары үшін: Басқару серверінен алынған деректер Google қызметтеріне беріледі. Бұл қосылым Android ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

11. Тек Android ұялы құрылғылары үшін: Google серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым ұялы құрылғыларға, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

12. Тек iOS ұялы құрылғылары үшін: iOS MDM серверінен алынған деректер Apple Push Notification серверлеріне жіберіледі. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

13. Тек iOS ұялы құрылғылары үшін: Apple серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым iOS ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

14. Тек мобильдік құрылғылар үшін: басқарылатын бағдарлама деректерді басқару серверіне 13292/13293 TLS порты арқылы тікелей немесе кері прокси-сервер көмегімен жібереді.

15. Тек ұялы құрылғылар үшін: ұялы құрылғыдан алынған деректер Kaspersky инфрақұрылымына беріледі.

    Мобильдік құрылғыда интернетке кіру рұқсаты болмаса, деректер басқару серверіне 17100 порты арқылы тасымалданады және басқару сервері оларды Kaspersky инфрақұрылымына жібереді; алайда бұл сценарий өте сирек қолданылады.

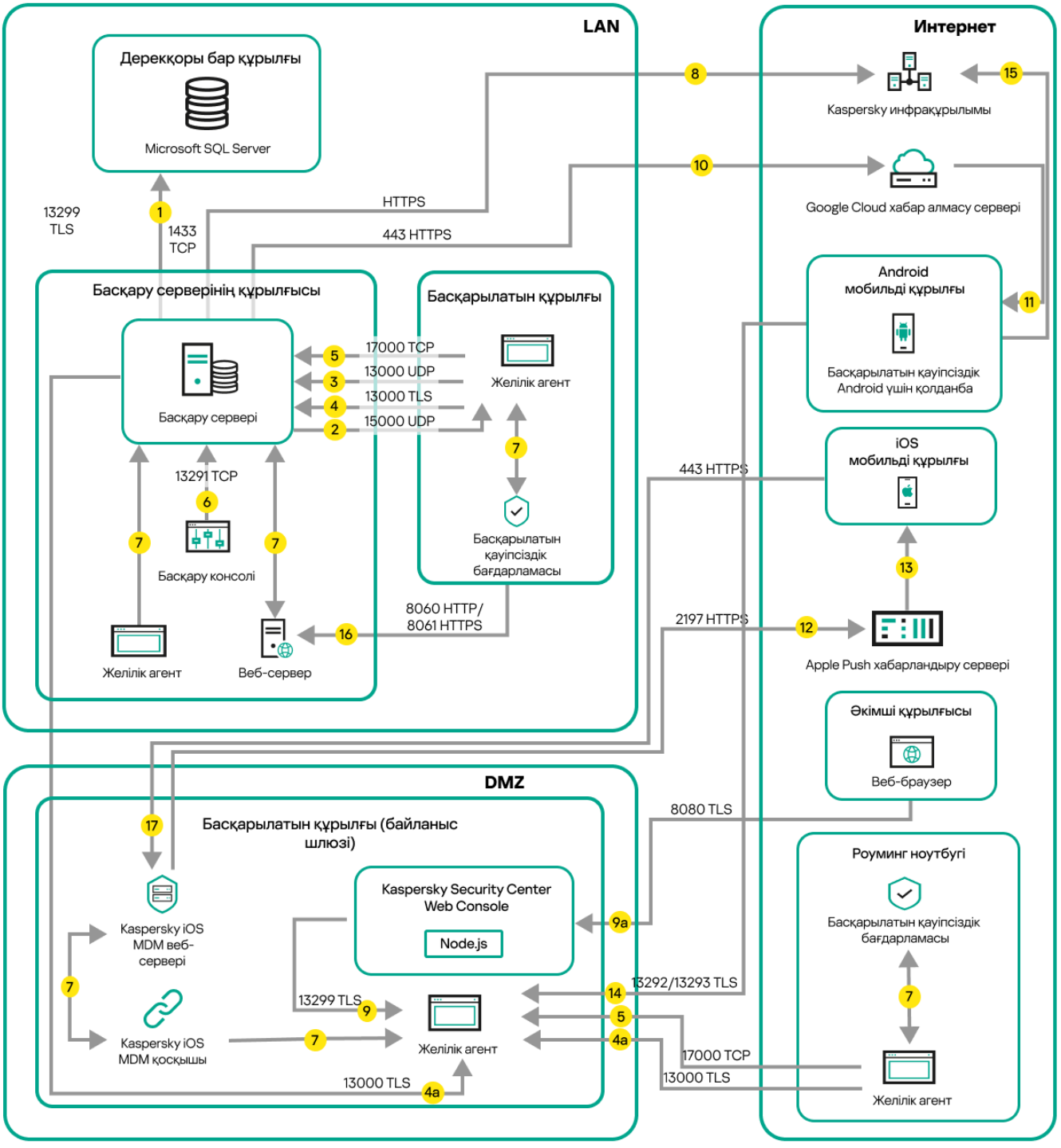
16. Басқарылатын құрылғылардан, соның ішінде ұялы құрылғылардан пакеттерге арналған сұраулар Басқару сервері орнатылған құрылғыда орналасқан Веб-серверге жіберіледі.

17. Тек iOS ұялы құрылғылары үшін: ұялы құрылғылардан алынған деректер 443 TLS порты арқылы Басқару сервері немесе қосылым шлюзі орнатылған құрылғыда орналасқан iOS MDM серверіне жіберіледі.

Жергілікті желі (LAN) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар; қосылым шлюзін қолдану

Төмендегі суретте, Басқару сервері жергілікті желі (LAN) ішінде, ал басқарылатын құрылғылар, сонымен қатар ұялы құрылғылар интернетте болатын деректер трафигі көрсетілген. Қосылым шлюзі қолданылуда.

Бұл орналастыру схемасы, ұялы құрылғылардың тікелей Басқару серверіне қосылғанын қаламасаңыз және кері прокси-сервер немесе корпоративтік брандмауэрді қолданғыңыз келмесе, ұсынылады.



Басқару серверіне қосылым шлюзі арқылы қосылған басқарылатын ұялы құрылғылар

Бұл суретте басқарылатын құрылғылар демилитаризацияланған аймақта (DMZ) орналасқан қосылым шлюзі арқылы Басқару серверіне қосылған. Кері прокси-сервер немесе корпоративтік желілік экран пайдаланылмайды.

Нұсқарлар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт немесе Microsoft SQL Server үшін 1433-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

   > Kaspersky Security Center бағдарламасының ерте нұсқаларында тарату нүктесі жаңарту агенті деп аталған.

   4а. Демилитаризацияланған аймақтағы қосылым шлюзі 13000 TLS порты арқылы Басқару серверінен қосылымды қабылдайды. Демилитаризацияланған аймақтағы қосылым шлюзі Басқару сервері порттарына кіре алмайтындықтан, Басқару сервері қосылым шлюзімен тұрақты сигнал байланысын жасайды және қолдайды. Сигнал қосылымы деректерді беру үшін пайдаланылмайды; ол тек желіге шақыру жіберу үшін қолданылады. Қосылым шлюзі Серверге қосылуы қажет болғанда, ол Серверге осы сигнал қосылымы арқылы хабарлайды, содан кейін Сервер деректерді беру үшін қажетті қосылым жасайды.

   Сыртқы құрылғылар қосылым шлюзіне 13000 TLS порты арқылы да қосылады.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. MMC негізіндегі басқару консолі деректері 13291 порты арқылы басқару серверіне тасымалданады. (Басқару консолін бір немесе басқа құрылғыға орнатуға болады.)

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   9a. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

10. Тек Android ұялы құрылғылары үшін: Басқару серверінен алынған деректер Google қызметтеріне беріледі. Бұл қосылым Android ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

11. Тек Android ұялы құрылғылары үшін: Google серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым ұялы құрылғыларға, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

12. Тек iOS ұялы құрылғылары үшін: iOS MDM серверінен алынған деректер Apple Push Notification серверлеріне жіберіледі. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

13. Тек iOS ұялы құрылғылары үшін: Apple серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым iOS ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

14. Тек мобильдік құрылғылар үшін: басқарылатын бағдарлама деректерді басқару серверіне 13292/13293 TLS порты арқылы тікелей немесе кері прокси-сервер көмегімен жібереді.

15. Тек ұялы құрылғылар үшін: ұялы құрылғыдан алынған деректер Kaspersky инфрақұрылымына беріледі.

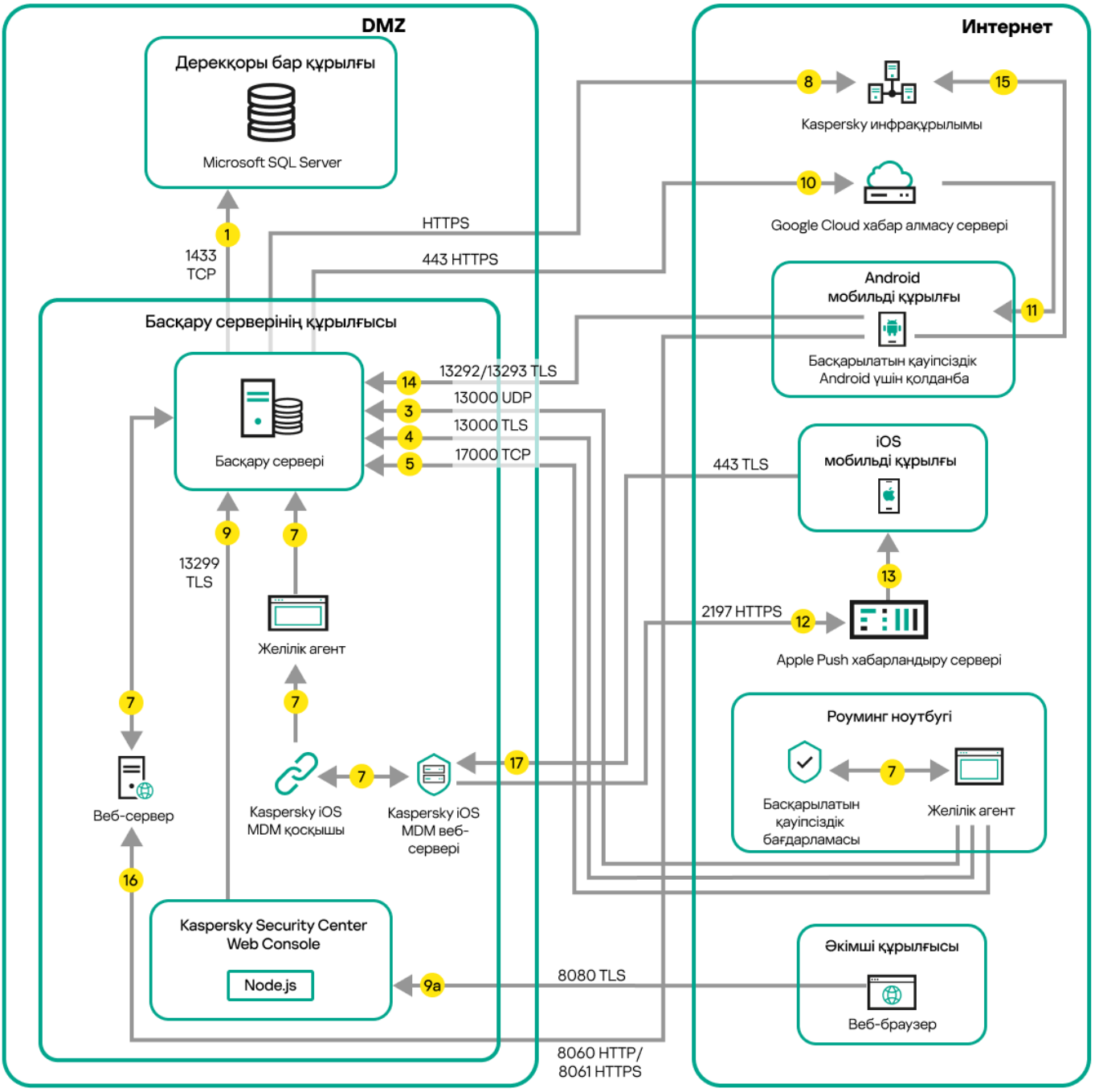
    Мобильдік құрылғыда интернетке кіру рұқсаты болмаса, деректер басқару серверіне 17100 порты арқылы тасымалданады және басқару сервері оларды Kaspersky инфрақұрылымына жібереді; алайда бұл сценарий өте сирек қолданылады.

16. Басқарылатын құрылғылардан, соның ішінде ұялы құрылғылардан пакеттерге арналған сұраулар Басқару сервері орнатылған құрылғыда орналасқан Веб-серверге жіберіледі.

17. Тек iOS ұялы құрылғылары үшін: ұялы құрылғылардан алынған деректер 443 TLS порты арқылы Басқару сервері немесе қосылым шлюзі орнатылған құрылғыда орналасқан iOS MDM серверіне жіберіледі.

Демилитаризацияланған аймақтың (DMZ) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар

Төмендегі суретте Басқару сервері демилитаризацияланған аймақта, ал ұялы құрылғыларды қоса алғанда, басқарылатын құрылғылар интернетте орналасқан деректер трафигі көрсетілген.



Демилитаризацияланған аймақтағы Басқару сервері, интернеттегі басқарылатын ұялы құрылғылары

Бұл суретте қосылым шлюзі пайдаланылмайды: ұялы құрылғылар Басқару серверіне тікелей қосылады.

Нұсқалар трафиктің бағытын көрсетеді: әрбір нұсқар қоңырауға "жауап беретін" құрылғыға қосылымды бастайтын құрылғыдан өткізілген. Деректерді беру үшін қолданылатын протоколдың атауы мен порт нөмірі көрсетілген. Әрбір нұсқар нөмірленген және тиісті деректер трафигі туралы келесі ақпаратты қамтиды:

1. Басқару сервері деректерді дерекқорға жібереді. Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт немесе Microsoft SQL Server үшін 1433-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2. Басқару серверімен байланысуға арналған сұраулар 15000 UDP порты арқылы барлық ұялы емес басқарылатын құрылғыларға жіберіледі.

   Желілік агенттер сұрауларды бір-біріне бір кеңінен тарататын домен шегінде жібереді. Содан соң, деректер Басқару серверіне жіберіледі және кеңінен тарататын доменнің шектерін анықтау үшін және тарату нүктелерін автоматты түрде тағайындау үшін қолданылады (бұл параметр қосулы болса).

   Басқару серверінің басқарылатын құрылғыларға тікелей қатынасы болмаса, Басқару серверінен осы құрылғыларға байланыс сұраулары тікелей жіберілмейді.

3. Басқарылатын құрылғыларды өшіру туралы ақпарат Желілік агенттен Басқару серверіне 13000 UDP порты арқылы беріледі.

4. Басқару сервері қосылымдарды Желілік агенттерден және қосалқы Басқару серверлерінен 13000 TLS порты арқылы қабылдайды.

   Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолдансаңыз, онда сіздің желіңізде Басқару сервері 14000 TLS порты арқылы Желілік агенттерден қосылымдарды қабылдай алады. Kaspersky Security Center нұсқасы да 14000-порт бойынша Желілік агенттерді қосуды қолдайды, бірақ 13000 TLS портын пайдалану ұсынылады.

   > Kaspersky Security Center бағдарламасының ерте нұсқаларында тарату нүктесі жаңарту агенті деп аталған.

5. Басқарылатын құрылғылар (ұялы құрылғылардан басқа) 17000 TCP порты арқылы белсендіруді сұрайды. Құрылғының интернетке өзіндік қатынасы болса, мұның қажеті жоқ; бұл жағдайда, құрылғы деректерді Kaspersky серверлеріне тікелей интернет арқылы жібереді.

6. MMC негізіндегі басқару консолі деректері 13291 порты арқылы басқару серверіне тасымалданады. (Басқару консолін бір немесе басқа құрылғыға орнатуға болады.)

7. Бір құрылғыдағы бағдарламалар жергілікті трафикпен алмасады (не Басқару серверінде, не басқарылатын құрылғыда). Сыртқы порттарды ашу қажет емес.

8. Басқару серверінен Kaspersky серверлеріне жіберілетін деректер (мысалы, KSN деректері, лицензиялар туралы ақпарат) және Kaspersky серверлерінен Басқару серверіне жіберілетін деректер (мысалы, бағдарламаларды жаңарту және антивирустық дерекқорларды жаңарту) HTTPS протоколы бойынша жіберіледі.

   Басқару серверіңізде интернетке қатысыңыздың болуын қаламасаңыз, осы деректерді қолмен басқаруыңыз керек.

9. Kaspersky Security Center Web Console сервері деректерді бірдей құрылғыда немесе басқасында орнатылуы мүмкін Басқару серверіне 13299 TLS-порты арқылы жібереді.

   9a. Жеке әкімші құрылғысында орнатылған браузерден алынған деректер TLS 8080 порты арқылы Kaspersky Security Center Web Console Server серверіне жіберіледі. Kaspersky Security Center Web Console Server серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

10. Тек Android ұялы құрылғылары үшін: Басқару серверінен алынған деректер Google қызметтеріне беріледі. Бұл қосылым Android ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

11. Тек Android ұялы құрылғылары үшін: Google серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым ұялы құрылғыларға, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

12. Тек iOS ұялы құрылғылары үшін: iOS MDM серверінен алынған деректер Apple Push Notification серверлеріне жіберіледі. Содан соң, push хабарландырулары ұялы құрылғыларға жіберіледі.

13. Тек iOS ұялы құрылғылары үшін: Apple серверлерінен келетін push хабарландырулары ұялы құрылғыға жіберіледі. Бұл қосылым iOS ұялы құрылғыларына, Басқару серверіне қосылуы қажет екендігі туралы хабарлау үшін қолданылады.

14. Тек мобильдік құрылғылар үшін: басқарылатын бағдарлама деректерді басқару серверіне 13292/13293 TLS порты арқылы тікелей немесе кері прокси-сервер көмегімен жібереді.

15. Тек ұялы құрылғылар үшін: ұялы құрылғыдан алынған деректер Kaspersky инфрақұрылымына беріледі.

    Мобильдік құрылғыда интернетке кіру рұқсаты болмаса, деректер басқару серверіне 17100 порты арқылы тасымалданады және басқару сервері оларды Kaspersky инфрақұрылымына жібереді; алайда бұл сценарий өте сирек қолданылады.

16. Басқарылатын құрылғылардан, соның ішінде ұялы құрылғылардан пакеттерге арналған сұраулар Басқару сервері орнатылған құрылғыда орналасқан Веб-серверге жіберіледі.

17. Тек iOS ұялы құрылғылары үшін: ұялы құрылғылардан алынған деректер 443 TLS порты арқылы Басқару сервері немесе қосылым шлюзі орнатылған құрылғыда орналасқан iOS MDM серверіне жіберіледі.

Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларының өзара әрекеттесуі: қосымша мәліметтер

Бұл бөлімде Kaspersky Security Center құрамындағы құрамдастар мен басқарылатын қауіпсіздік бағдарламалары арасындағы өзара әрекеттесу схемалары берілген. Схемаларда, қолжетімді болуы керек порт нөмірлері және порттарды ашатын процестердің атауы көрсетіледі.

Өзара әрекеттесу схемаларындағы шартты белгілер

Төмендегі кестеде, схемаларда қолданылған шартты белгілер келтірілген.

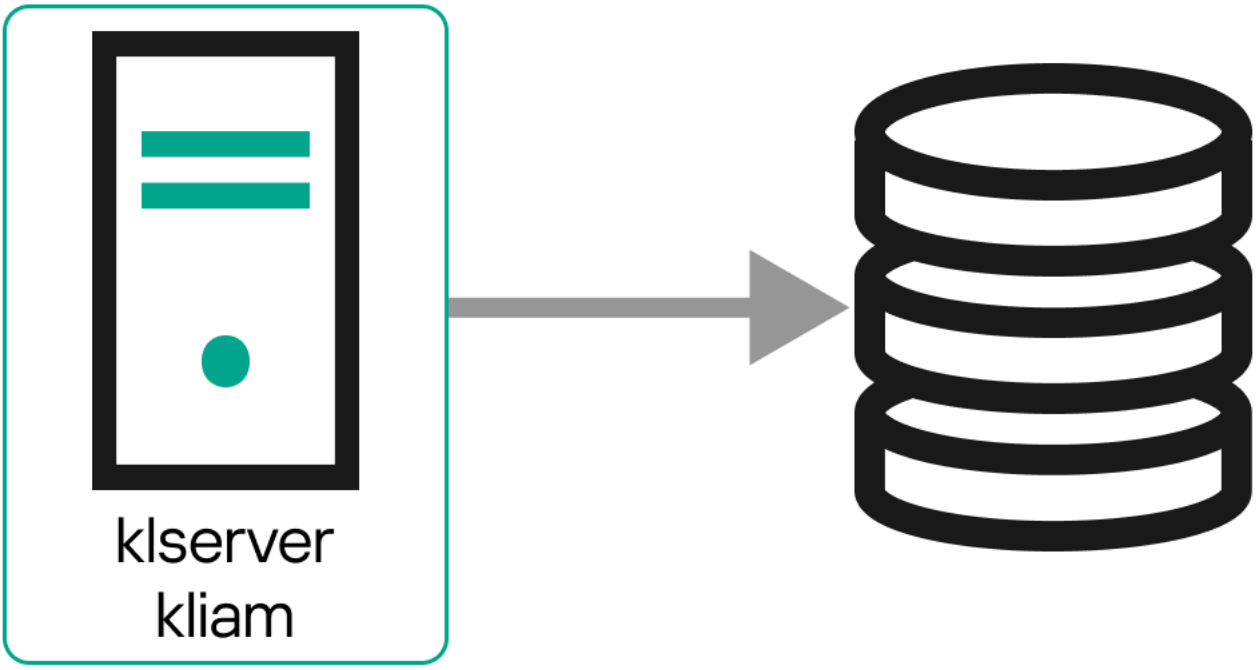
Шартты белгілер

Белгіше	Мән
	Басқару сервері

	Қосалқы Басқару сервері
	ДҚБЖ
	Желілік агент және Kaspersky Endpoint Security отбасының бағдарламасы (немесе Kaspersky Security Center басқара алатын басқа қауіпсіздік бағдарламасы) орнатылған клиент құрылғысы
	Қосылым шлюзі
	Тарату нүктесі
	Kaspersky Security for Mobile бағдарламасы орнатылған ұялы клиент құрылғысы
	Пайдаланушының құрылғысындағы браузер
	Құрылғыда іске қосылған және кез келген портты ашатын процесс
	Порт және оның нөмірі
	TCP трафигі (меңзер бағыты трафик бағытын білдіреді)
	TCP трафигі (меңзер бағыты трафик бағытын білдіреді)
	COM шақыру
	ДҚБЖ тасымалдау
	Демилитаризацияланған аймақ шекаралары

Басқару сервері және ДҚБЖ

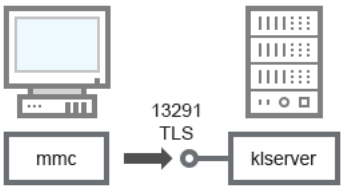
Деректер Басқару серверінен SQL Server, MySQL немесе MariaDB дерекқорына түседі.



Басқару сервері және ДҚБЖ

Басқару сервері мен дерекқорды әртүрлі құрылғыларға орнатқан болсаңыз, дерекқор орналасқан құрылғыдағы қажетті порттарды (мысалы, MySQL Server үшін 3306-порт немесе Microsoft SQL Server үшін 1433-порт) қолжетімді етуіңіз қажет. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

Басқару сервері және Басқару консолі



Басқару сервері және Басқару консолі

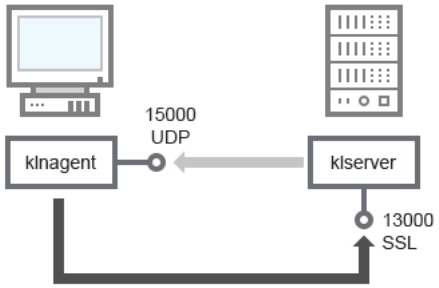
Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері және Басқару консолі (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Басқару сервері	13291	klserver	TCP	Иә	Басқару консолінен қосылымдар қабылдау

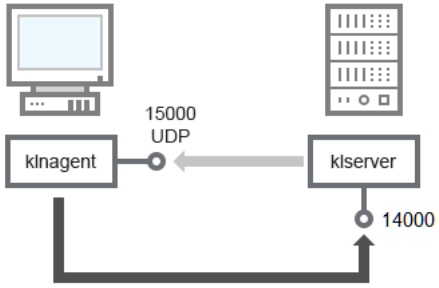
Басқару сервері және клиент құрылғысы: Қауіпсіздік бағдарламасын басқару

Басқару сервері 13000 қорғалған порты бойынша Желілік агенттерден қосылымдарды қабылдайды (төмендегі суретті қараңыз).



Басқару сервері және клиент құрылғысы: қауіпсіздік бағдарламасын басқару, 13000-порт арқылы қосылу (ұсынылады)

Егер сіз Kaspersky Security Center бағдарламасының алдыңғы нұсқаларының бірін қолданған болсаңыз, онда сіздің желіңізде Басқару сервері 14000 қорғалмаған порты арқылы Желілік агенттерден қосылымдарды қабылдай алады (төмендегі суретті қараңыз). Kaspersky Security Center 15.1 нұсқасы 14000-порт бойынша желілік агенттерді қосуды қолдайды, бірақ қорғалған 13000-портты пайдалану ұсынылады.



Басқару сервері және клиент құрылғысы: қауіпсіздік бағдарламасын басқару, 14000-порт арқылы қосылу (төмен қорғаныс)

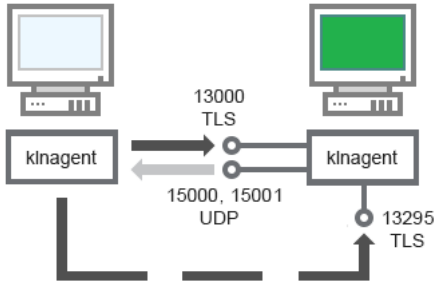
Схемаларға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері және клиент құрылғысы: Қауіпсіздік бағдарламасын басқару (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS (TCP үшін ғана)	Портты тағайындау
Желілік агент	15000	klnagent	UDP	Мәні жоқ	Желілік агенттерге арналған көп мекенжайлы таратылым
Басқару сервері	13000	klserver	TCP	Иә	Желілік агенттерден қосылымдар қабылдау
Басқару сервері	14000	klserver	TCP	Жоқ	Желілік агенттерден қосылымдар қабылдау

Тарату нүктесін пайдаланып клиент құрылғысындағы бағдарламалық жасақтаманы жаңарту

Клиент құрылғысы тарату нүктесіне 13000-порт арқылы, ал сіз тарату нүктесін push сервері ретінде пайдалансаңыз, 13295-порт арқылы қосылады; тарату нүктесі 15000-порт арқылы Желілік агенттерге көп мекенжайлы таратылым жібереді (төмендегі суретті қараңыз). Жаңартулар мен орнату пакеттері тарату нүктесінен 15001 порты арқылы алынады.



Тарату нүктесін пайдаланып клиент құрылғысындағы бағдарламалық жасақтаманы жаңарту

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Тарату нүктесі арқылы бағдарламалық жасақтаманы жаңарту (трафик)

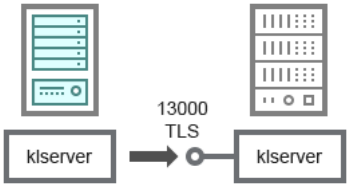
Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS (TCP үшін ғана)	Портты тағайындау
Желілік агент	15000	klnagent	UDP	Мәні жоқ	Желілік агенттерге арналған көп мекенжайлы таратылым
Желілік агент	15001	klnagent	UDP	Мәні жоқ	Тарату нүктесінен жаңартулар мен орнату пакеттерін алу
Тарату нүктесі	13000	klnagent	TCP	Иә	Желілік агенттерден қосылымдар қабылдау
Тарату нүктесі	13295	klnagent	TCP	Иә	Клиент құрылғыларынан қосылымдарды қабылдау (push сервері арқылы)

Басқару серверлерінің иерархиясы: негізгі Басқару сервері және қосалқы Басқару сервері

Схемада (төмендегі суретті қараңыз), 13000-порт иерархияға біріктірілген Басқару серверлерінің өзара әрекеттесуі үшін қалай қолданылатынын көрсетеді.

Серверлерді иерархияға біріктіру кезінде екі Сервердің 13291-порты қолжетімді болуы керек. 13291-порт арқылы Басқару консолі Басқару серверіне қосылады.

Алдағыда, Серверлерді иерархияға біріктіргеннен кейін, сіз екі Серверді де негізгі Басқару серверіне қосылған Басқару консолі арқылы басқара аласыз. Осылайша, тек басты Сервердің 13291-порты қолжетімді болуы керек.



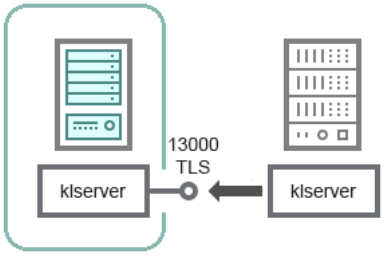
Басқару серверлерінің иерархиясы: негізгі Басқару сервері және қосалқы Басқару сервері

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару серверлерінің иерархиясы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Негізгі Басқару сервері	13000	klserver	TCP	Иә	Қосалқы Басқару серверлерінен қосылымдарды қабылдау

Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы



Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы

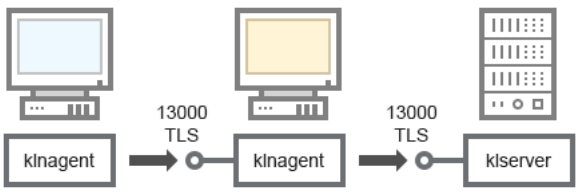
Схемада Басқару серверлерінің иерархиясы көрсетілген, онда демилитаризацияланған аймақтағы қосалқы Сервер басты Серверден қосылымды қабылдайды (схемаға түсініктемелер алу үшін төмендегі кестені қараңыз). Серверлерді иерархияға біріктіру кезінде екі Сервердің 13291-порты қолжетімді болуы керек. 13291-порт арқылы Басқару консолі Басқару серверіне қосылады.

Алдағыда, Серверлерді иерархияға біріктіргеннен кейін, сіз екі Серверді де негізгі Басқару серверіне қосылған Басқару консолі арқылы басқара аласыз. Осылайша, тек басты Сервердің 13291-порты қолжетімді болуы керек.

Демилитаризацияланған аймақта қосалқы Сервері бар Басқару серверлері иерархиясы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Қосалқы Басқару сервері	13000	klserver	TCP	Иә	Негізгі Басқару серверінен қосылымдарды қабылдау

Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы



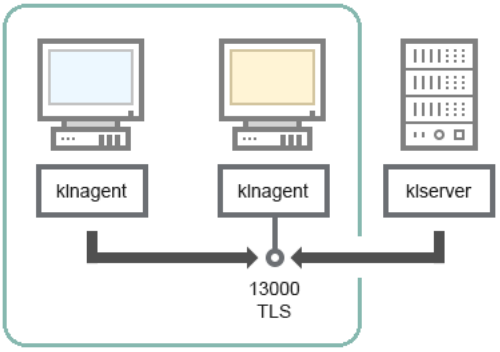
Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Басқару сервері	13000	klserver	TCP	Иә	Желілік агенттерден қосылымдар қабылдау
Желілік агент	13000	klnagent	TCP	Иә	Желілік агенттерден қосылымдар қабылдау

Басқару сервері және демилитаризацияланған аймағы екі құрылғы: қосылымдар шлюзі және клиент құрылғысы



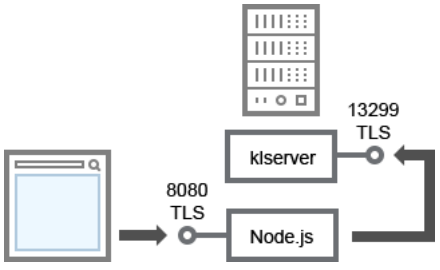
Демилитаризацияланған аймақтағы Басқару сервері, қосылымдар шлюзі және клиент құрылғысы

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері, желі сегментіндегі қосылымдар шлюзі және клиент құрылғысы (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Желілік агент	13000	klnagent	TCP	Иә	Желілік агенттерден қосылымдар қабылдау

Басқару сервері және Kaspersky Security Center Web Console



Басқару сервері және Kaspersky Security Center Web Console

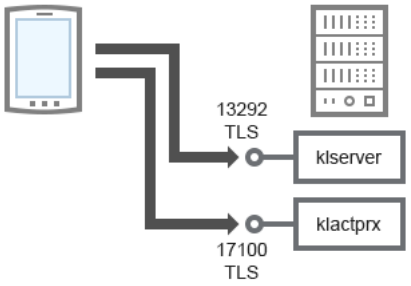
Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Басқару сервері және Kaspersky Security Center Web Console (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Басқару сервері	13299	klserver	TCP	Иә	Kaspersky Security Center Web Console веб-консолінен OpenAPI арқылы Басқару серверіне қосылымдар алу
Kaspersky Security Center Web Console сервері немесе Басқару сервері	8080	Node.js: серверлік JavaScript	TCP	Иә	Kaspersky Security Center Web Console серверінен қосылымдар алу

Kaspersky Security Center Web Console серверін Басқару сервері орнатылған құрылғыға немесе басқа құрылғыға орнатуға болады.

Ұялы құрылғыда қауіпсіздік қолданбасын белсендіру және басқару



Ұялы құрылғыда қауіпсіздік қолданбасын белсендіру және басқару

Схемаға түсініктемелер алу үшін төмендегі кестені қараңыз.

Ұялы құрылғыда қауіпсіздік қолданбасын белсендіру және басқару (трафик)

Құрылғы	Порт нөмірі	Портты ашатын процесс атауы	Протокол	TLS	Портты тағайындау
Басқару сервері	13292	klserver	TCP	Иә	Басқару консолінен Басқару серверіне қосылымдар қабылдау
Басқару сервері	17100	klactprx	TCP	Иә	Ұялы құрылғылардан қолданбаларды белсендіру үшін қосылымдарды қабылдау

Үздік енгізу практикалары

Kaspersky Security Center бағдарламасы таратылған бағдарлама болып саналады. Kaspersky Security Center құрамына келесі бағдарламалар кіреді:

- Басқару сервері – ұйымның құрылғыларын басқару және деректерді ДҚБЖ-де сақтау үшін жауапты орталық құрамдас.
- Басқару консолі – әкімшінің негізгі құралы. Басқару консолі Басқару серверімен бірге жеткізіледі, бірақ әкімшінің бір немесе бірнеше құрылғысына бөлек орнатылуы мүмкін.
- Желілік агент – құрылғыда орнатылған қауіпсіздік бағдарламасын басқару, сондай-ақ құрылғы туралы ақпаратты алу және осы ақпаратты Басқару серверіне жіберу үшін қолданылады. Желілік агенттер ұйымның құрылғыларына орнатылады.

Kaspersky Security Center бағдарламасын ұйымның желісінде орналастыру келесі тәсілдермен жүзеге асырылады:

- Басқару серверін орнату;
- Басқару консолін әкімшінің құрылғысына орнату;
- Желілік агент пен қауіпсіздік бағдарламаларын ұйымның құрылғыларына орнату.

Қорғанысты күшейту нұсқаулығы

Kaspersky Security Center бағдарламасы ұйымның желісін қорғау жүйесін басқару және қызмет көрсету жөніндегі негізгі тапсырмаларды орталықтандырылған шешуге арналған. Қолданба әкімшіге ұйым желісінің қауіпсіздік деңгейі туралы егжей-тегжейлі ақпаратқа қол жеткізуге мүмкіндік береді. Kaspersky Security Center, Kaspersky бағдарламаларына негізделген барлық қорғаныс құрамдастарын конфигурациялауға мүмкіндік береді.

Kaspersky Security Center Басқару сервері клиент құрылғыларының қорғанысын басқаруға толық қатынасу мүмкіндігіне ие және ұйымның қорғаныс жүйесінің маңызды құрамдас бөлігі болып табылады. Сондықтан, Басқару сервері үшін күшейтілген қорғаныс шаралары қажет.

Конфигурациялау алдында басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын пайдаланып, Kaspersky Security Center басқару серверінің сақтық көшірмесін жасаңыз және оны қауіпсіз жерде сақтаңыз.

Қорғанысты күшейту нұсқаулығы, бұзылу қаупін азайту үшін Kaspersky Security Center және оның құрамдастарын конфигурациялаудың ұсыныстары мен ерекшеліктерін сипаттайды.

Қорғанысты күшейту нұсқаулығы келесі ақпаратты қамтиды:

- Басқару серверін орналастыру схемасын таңдау
- Басқару серверіне қауіпсіз қосылымды конфигурациялау
- Басқару серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау
- Басқару серверін қорғауды басқару
- Клиент құрылғыларын қорғауды басқару
- Басқарылатын қолданбалар қорғанысын конфигурациялау
- Басқару серверіне техникалық қызмет көрсету
- Үшінші тарап жүйелеріне ақпарат беру
- Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар

Басқару серверін орналастыру

Басқару сервері архитектурасы

Жалпы алғанда, басқарудың орталықтандырылған архитектурасын таңдауға қорғалатын құрылғылардың орналасуы, іргелес желілерден қатынасу, дерекқорларды жаңарту схемалары және басқа параметрлер әсер етеді.

Архитектураны дамытудың бастапқы кезеңінде Kaspersky Security Center құрамдастарымен және олардың бір-бірімен өзара әрекеттесуімен, сондай-ақ деректер трафигі және портты пайдалану схемаларымен танысуды ұсынамыз.

Осы ақпарат негізінде мыналарды анықтайтын архитектураны қалыптастыру қажет:

- Басқару серверінің орналасуы және желіге қосылуы
- Әкімшілердің жұмыс станцияларын ұйымдастыру және Басқару серверіне қосылу тәсілдері
- Желілік агент және қорғау бағдарламасын орнату тәсілі
- Тарату нүктелерін пайдалану
- Виртуалды Басқару серверлерін қолдану
- Басқару серверлерінің иерархиясын қолдану
- Антивирустық дерекқорларды жаңарту схемасы
- Басқа ақпарат ағындары

Басқару сервері үшін құрылғыны таңдау

Басқару серверін инфрақұрылымдағы арнайы серверге орнату ұсынылады. Серверде үшінші тарап бағдарламалық жасақтамасы болмаса, бұл Kaspersky Security Center талаптарын ескере отырып және үшінші тарап бағдарламалық жасақтамасының талаптарына тәуелді болмай, қауіпсіздік параметрлерін конфигурациялауға мүмкіндік береді.

Басқару серверін физикалық серверде де, виртуалды машинада да орналастыруға болады. Таңдалған құрылғы аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз.

Басқару серверінің орналасуы

Басқару сервері басқаратын құрылғыларды осында орналастыруға болады:

- желінің жергілікті сегментінде;
- интернетте;
- демилитаризацияланған аймақта (DMZ).

Бұл жағдайда, Басқару сервері келесі сегменттерде де орналасуы мүмкін: демилитаризацияланған аймақтың (DMZ) технологиялық, корпоративтік сегменттерінде.

Желінің оқшауланған сегментін қорғауды басқару үшін Kaspersky Security Center пайдаланған кезде, Басқару серверін демилитаризацияланған аймақ (DMZ) сегментінде орналастыру ұсынылады. Бұл, құрылғыларды басқару және жаңартуларды жеткізу мүмкіндігін сақтай отырып, желілердің толыққанды сегменттелуін ұйымдастыруға және қорғалатын сегментке ықтимал жүгінуді азайтуға мүмкіндік береді.

Басқару серверін домен контроллеріне, терминал серверіне немесе пайдаланушы құрылғысына орнатуды шектеу

Басқару серверін домен контроллеріне, терминал серверіне немесе пайдаланушы құрылғысына орнату мүлдем ұсынылмайды.

Желінің өзекті құрылғыларын функционалдық бөлуді көздеу ұсынылады. Бұл, құрылғы істен шыққанда немесе бұзылған кезде әртүрлі жүйелердің жұмыс істеу қабілетін сақтауға мүмкіндік береді. Сонымен қатар, бұл тәсілдеме әр құрылғы үшін әртүрлі қауіпсіздік саясатын жүзеге асыруға мүмкіндік береді.

Мысалы, домен контроллеріне қолданылатын қауіпсіздік шектеулері, Басқару серверінің өнімділігін айтарлықтай төмендетіп, оның кейбір функцияларын пайдалануды мүмкін етпеуі мүмкін. Егер шабуылдаушы домен контроллеріне артықшылықты қатынасқа ие болса, олар Active Directory Domain Services (AD DS) дерекқорын өзгерте алады, бұза алады немесе жоя алады. Сонымен қатар, Active Directory басқаратын барлық жүйелер мен есептік жазбалар бұзылады.

Басқару серверін орнату және іске қосу үшін есептік жазбалар

Басқару серверінің дерекқорына қатынасу үшін домен есептік жазбаларын пайдаланбау үшін Басқару серверін орнатуды жергілікті әкімші есептік жазбасы астында іске қосу ұсынылады. Қажетті есептік жазбалар жиынтығы және олардың құқықтары таңдалған ДҚБЖ түріне, ДҚБЖ орналасқан жеріне және Басқару серверінің дерекқорын құру тәсіліне байланысты.

KLAdmins және KLOperators пайдаланушы топтары Kaspersky Security Center орнату кезінде автоматты түрде жасалады. Бұл топтарға Басқару серверіне қосылу және оның нысандарымен жұмыс істеу құқығы беріледі.

Kaspersky Security Center бағдарламасы қандай есептік жазба арқылы орнатылып жатқанына қарамастан, KLAdmins және KLOperators топтары келесідей құрылады:

- Орнату доменге кіретін пайдаланушы есептік жазбасы астында орындалса, топтар Басқару сервері бар құрылғыда және Басқару сервері бар құрылғыны қамтитын доменде жасалады.
- Егер орнату жүйенің есептік жазбасында жүргізілсе, топтар тек Басқару сервері бар құрылғыда ғана құрылады.

Доменде KLAdmins және KLOperators топтарын құруды және соның нәтижесінде **ол орнатылған құрылғыдан тыс Басқару серверін басқару құқығын беруді** болдырмау үшін жергілікті есептік жазба астында Kaspersky Security Center орнату ұсынылады.

Басқару серверін орнату кезінде, Басқару сервері қызмет ретінде іске қосылатын есептік жазбаны таңдаңыз. Әдепкі бойынша қолданба Басқару серверінің қызметі (klserver) іске қосылатын жергілікті KL-AK-* есептік жазбасын жасайды.

Қажет болса, Басқару сервері қызметін таңдалған есептік жазбадан іске қосуға болады. Бұл жағдайда, есептік жазбада ДҚБЖ-ға қосылу үшін әртүрлі құқықтар болуы керек. Қауіпсіздікті қамтамасыз ету үшін Басқару сервері қызметін іске қосу үшін артықшылықсыз есептік жазбаны пайдаланыңыз.

Басқару серверінің есептік жазбасы үшін қате қатынасу параметрлерін болдырмау үшін оны автоматты түрде жасау ұсынылады.

Басқару серверін доменнен шығару

Маңызды жүйелер құрылғыларының топтарын қорғау үшін басқару серверін пайдалансаңыз, доменге басқару серверінің құрылғысын қосу ұсынылмайды. Бұл сізге Kaspersky Security Center басқару құқықтарын ажыратуға және домен бұзылған жағдайда басқаруға қол жеткізуді болдырмауға мүмкіндік береді.

Басқару серверін жұмыс тобының бөлігі болып табылатын құрылғыға орнатсаңыз, басқару серверімен жұмыс істеудің келесі сценарийлері қолжетімді болмайтынын ескеріңіз:

- Ақауларға төзімді Kaspersky Security Center кластерін пайдалану.
- Ақауларға төзімді Windows Server кластерін пайдалану.
- Windows жүйесіне арналған SQL Server серверін бөлек құрылғыда пайдалану

  Басқару сервері мен SQL Server бір доменге немесе сенімді доменге қосылған жағдайда ғана, Windows жүйесіне арналған SQL серверін бөлек құрылғыда пайдалануға болады. Басқару сервері, SQL сервері және сақтық көшірмелерге арналған ортақ UNC жұмыс тобында болса, SQL сервері мен бөлісу арасында қол жеткізу және оқу-жазу құқықтарын қауіпсіз орната алмайсыз.
- Active Directory топтық саясаттары көмегімен Басқару серверінің құралдарымен қашықтан орнату

Басқару серверін Active Directory доменінен ажырату қажет болса, Kaspersky Security Center Басқару серверінің атауын қалай өзгертуге болады бөлімінде сипатталған қадамдарды орындаңыз.

Жұмыс тобының бөлігі болып табылатын құрылғыға басқару серверін орнату қажет болса, Kaspersky Security Center Windows орнына Kaspersky Security Center Linux жүйесін пайдалануға да болады.

Қосылым қауіпсіздігі

TLS пайдалану

Басқару серверіне қауіпсіз емес қосылымдарға тыйым салу ұсынылады. Мысалы, Басқару серверін конфигурациялау кезінде HTTP протоколы арқылы Басқару серверіне қосылымдарды қоспау ұсынылады.

Басқару серверінің кейбір HTTP порттары әдепкі бойынша жабық екенін ескеріңіз. Қалған портты Kaspersky Security Center веб-сервері (8060) пайдаланады. Бұл портты Басқару сервері бар құрылғының желілік экран параметрлері арқылы шектеуге болады.

Қатаң TLS параметрлері

TLS 1.2 немесе одан жоғары нұсқасын пайдалану және қауіпсіз емес шифрлау алгоритмдерін пайдалануды шектеу немесе өшіру ұсынылады.

Басқару сервері пайдаланатын шифрлау протоколдарын (TLS) конфигурациялауға болады. Бұл ретте, Басқару серверінің белгілі бір нұсқасын шығару кезінде деректерді қауіпсіз тасымалдауды қамтамасыз ету үшін әдепкі бойынша шифрлау протоколының параметрлері конфигурацияланатынын есте сақтаңыз.

Windows есептік жазбаларымен қашықтан түпнұсқалық растамаға тыйым салу

Қашықтағы мекенжайлардан SSPI қосылымдарына тыйым салу LP_RestrictRemoteOsAuth арнайы жалаушасы арқылы мүмкін болады. Бұл жалауша жергілікті немесе домендегі Windows есептік жазбаларына арналған Басқару серверінде қашықтан түпнұсқалық растамаға тыйым салуға мүмкіндік береді.

Қашықтағы мекенжайлардан SSPI қосылымдарын шектеу үшін LP_RestrictRemoteOsAuth жалаушасын ауыстыру үшін:

1. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. LP_RestrictRemoteOsAuth жалаушасының мәнін көрсету үшін пәрмен жолында келесі пәрменді орындаңыз:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Басқару сервері қызметін қайта іске қосыңыз.

LP_RestrictRemoteOsAuth жалаушасы, қашықтан түпнұсқалық растама Kaspersky Security Center Web Console веб-консолі арқылы немесе Басқару серверімен бір құрылғыда орнатылған Басқару консолі арқылы орындалса жұмыс істемейді.

Басқару сервері дерекқорына қатынасуды шектеу

Басқару сервері дерекқорына қатынасуды шектеу ұсынылады. Мысалы, Басқару сервері бар құрылғыдан ғана қатынасуға рұқсат бере аласыз. Бұл белгілі осалдықтар арқылы Деректерді басқару серверінің дерекқорын бұзу ықтималдығын азайтады.

Параметрлерді пайдаланылатын дерекқордың пайдалану нұсқаулығына сәйкес конфигурациялауға, сондай-ақ желілік экрандарда жабық порттарды көздеуге болады.

Microsoft SQL Server түпнұсқалық растамасы

Microsoft SQL Server серверін Басқару серверінің ДҚБЖ ретінде пайдалансаңыз, дерекқорға тасымалданатын немесе одан алынатын Kaspersky Security Center деректерін, сондай-ақ осы дерекқорда сақталған деректерді рұқсатсыз қатынасудан қорғау керек. Ол үшін Kaspersky Security Center және SQL Server арасындағы қауіпсіз қосылымды қамтамасыз ету қажет. Қауіпсіз байланысты қамтамасыз етудің ең сенімді тәсілі - Kaspersky Security Center бағдарламасы мен SQL Server серверін бір құрылғыда орнату және екі бағдарлама үшін де бірлескен жад механизмін қолдану. Барлық жағдайларда, SQL Server үлгісінің түпнұсқалық растамасы үшін SSL/TLS сертификатын пайдалану ұсынылады.

Әдетте басқару сервері SQL серверіне келесі провайдерлер арқылы хабарласа алады:

- TCP/IP немесе Named Pipes қолданатын SQLOLEDB

  Бұл провайдер Windows операциялық жүйесіне орнатылған және әдепкі бойынша пайдаланылады.

- TCP/IP, Named Pipes немесе ортақ жад қолданатын MSOLEDBSQL

  Бұл провайдерді пайдаланғыңыз келсе, оны басқару сервері бар құрылғыға орнатуыңыз және `KLDBADO_UseMSOLEDBSQL` жаһандық орта айнымалысы үшін `1` мәнін орнатуыңыз қажет.

- TCP/IP, Named Pipes немесе ортақ жад қолданатын MSOLEDBSQL19

  Бұл провайдерді қолданғыңыз келсе, оны басқару сервері бар құрылғыға орнатып, `KLDBADO_UseMSOLEDBSQL` жаһандық орта айнымалысына `1` мәнін, ал `KLDBADO_ProviderName` жаһандық орта айнымалысына `MSOLEDBSQL19` мәнін орнатуыңыз қажет.

Сондай-ақ TCP/IP, Named Pipes немесе ортақ жад пайдаланар алдында қажетті протоколдың қосылғанына көз жеткізіңіз.

Сыртқы ДҚБЖ-мен өзара әрекет қауіпсіздігі

Басқару серверін (сыртқы ДҚБЖ) орнату кезінде ДҚБЖ бөлек құрылғыға орнатылса, осы ДҚБЖ-мен қауіпсіз өзара әрекет жасау және аутентификация үшін параметрлерді конфигурациялау ұсынылады. SSL аутентификациясын конфигурациялау туралы қосымша ақпаратты PostgreSQL серверінің аутентификациясы және Сценарий: MySQL серверінің аутентификациясы бөлімдерінен қараңыз.

Басқару серверіне қосылуға арналған рұқсат етілген IP мекенжайлары тізімін конфигурациялау

Әдепкісінше Kaspersky Security Center пайдаланушылары Kaspersky Security Center жүйесіне MMC негізіндегі басқару сервері, Kaspersky Security Center Web Console немесе OpenAPI қолданбалары орнатылған кез келген құрылғыдан кіре алады. Басқару серверін, пайдаланушылар оған тек рұқсат етілген IP мекенжайлары бар құрылғылардан қосыла алатындай етіп конфигурациялауға болады. Мысалы, қаскүнем рұқсат тізімінде жоқ құрылғыға орнатылған Kaspersky Security Center Web Console Server арқылы Kaspersky Security Center жүйесіне қосылуға әрекеттенген кезде, ол Kaspersky Security Center жүйесіне кіре алмайды.

Kaspersky Security Center Web Console-ге қосылу үшін IP мекенжайларының рұқсат тізімін конфигурациялау

Әдепкісінше Kaspersky Security Center пайдаланушылары Kaspersky Security Center Web Console-ге кез келген құрылғыдан қосыла алады. Kaspersky Security Center Web Console бар құрылғыда пайдаланушылар Kaspersky Security Center Web Console-ге тек рұқсат етілген IP мекенжайлары арқылы қосыла алуы үшін, желілік экранды (операциялық жүйеге немесе үшінші тарапқа орнатылған) конфигурациялау керек.

Сауалнама кезінде домен контроллеріне қосылу қауіпсіздігі

Басқару сервері немесе Linux тарату нүктесі домен контроллеріне сауалнама жүргізу үшін LDAPS арқылы қосылады. Әдепкісінше қосылу кезінде сертификатты растау қажет болмайды. Сертификатты растау процесін енгізу үшін `KLNAG_LDAP_TLS_REQCERT` жалаушасын 1-ге орнатыңыз. Сондай-ақ `KLNAG_LDAP_SSL_CACERT` жалауын пайдалану арқылы сертификаттар тізбегіне кіру үшін сертификат орталығына (CA) апаратын арнаулы жолды көрсетуге болады.

Есептік жазбалар және авторизация

Төмендегі қадамдарды орындамай тұрып, басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын пайдаланып, Kaspersky Security Center басқару серверінің сақтық көшірмесін жасаңыз және оны қауіпсіз жерде сақтаңыз.

Басқару серверін екі қадамдық тексеруді пайдалану

Kaspersky Security Center бағдарламасы Kaspersky Security Center Web Console және басқару консолі пайдаланушыларына RFC 6238 (TOTP: уақытқа негізделген бір реттік құпиясөз алгоритмі) негізінде екі қадамдық растауды пайдалануға мүмкіндік береді.

Егер сіздің есептік жазбаңызға екі қадамдық тексеру қосылса, Kaspersky Security Center Web Console немесе Басқару консолін кірген сайын пайдаланушы атыңызды, құпиясөзіңізді және қосымша бір реттік қауіпсіздік кодын енгізесіз. Егер сіз өзіңіздің есептік жазбаңыз үшін домендік түпнұсқалық растаманы қолдансаңыз, сізге қосымша бір реттік қауіпсіздік кодын енгізу қажет. Бір реттік қауіпсіздік кодын алу үшін, сіз өзіңіздің компьютеріңізге немесе ұялы құрылғыға аутентификация қолданбасын орнатуыңыз керек.

RFC 6238 стандартын қолдайтын бағдарламалық және аппараттық аутентификаторлар (токендер) бар. Мысалы, бағдарламалық аутентификаторларға Google Authenticator, Microsoft Authenticator, FreeOTP кіреді.

Басқару серверіне қосылатын сол құрылғыда аутентификация қолданбасын орнату мүлдем ұсынылмайды. Мысалы, ұялы құрылғыға аутентификация қолданбасын орнатуға болады.

Жаңа пайдаланушыларға екі сатылы растауды өз бетінше орнатуға тыйым салу

Kaspersky Security Center Web Console арнайы мүмкіндіктер қауіпсіздігін одан әрі жақсарту үшін мына әрекеттерді орындай аласыз

жаңа пайдаланушылардың екі сатылы растауды өз бетінше орнатуына тыйым салу.

Бұл опция қосылса, жаңа домен әкімшісі сияқты екі сатылы растауы өшірілген пайдаланушы екі сатылы растауды өз бетінше конфигурациялай алмайды. Демек мұндай пайдаланушыны басқару серверінде аутентификациялау мүмкін емес және ол екі қадамдық растау қосылған басқа Kaspersky Security Center әкімшісінің мақұлдауынсыз Kaspersky Security Center Web Console жүйесіне кіре алмайды.

Екі факторлы операциялық жүйе түпнұсқалық растамасын пайдалану

Мүмкіндігінше, Басқару сервері бар құрылғыда түпнұсқалық растама үшін токен, смарт-карта немесе басқа тәсіл арқылы көп факторлы түпнұсқалық растаманы (MFA) пайдалану ұсынылады.

Әкімші құпиясөзін сақтауға тыйым салу

Басқару консолін пайдаланған кезде әкімші құпиясөзін Басқару серверіне қосылу үшін диалогтық терезеде сақтау ұсынылмайды.

Сондай-ақ, Kaspersky Security Center Web Console веб-консолі арқылы Басқару серверімен жұмыс істегенде, пайдаланушы құрылғысындағы браузерде әкімші құпиясөзін сақтау ұсынылмайды.

Ішкі пайдаланушы авторизациясы

Әдепкі бойынша Басқару серверінің ішкі пайдаланушы есептік жазбасының құпиясөзі келесі талаптарға сай болуы керек:

- Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Құпиясөзді енгізу әрекеттерінің санын өзгерте аласыз.

Kaspersky Security Center пайдаланушысы құпиясөзді шектеулі рет енгізе алады. Осыдан кейін, пайдаланушы есептік жазбасы бір сағатқа бұғатталады.

Ішкі пайдаланушы есептік жазбасының құпиясөзін өзгерту опцияларын конфигурациялау

Ішкі пайдаланушы есептік жазбасының құпиясөзін өзгерту үшін келесі опцияларды конфигурациялауды ұсынамыз:

- Құпиясөзді ауыстыру кезеңі
- Құпиясөзді өзгерту қажеттігі туралы алдын ала көрсетілетін ескерту уақыты
- **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** опциясының мәні

Есептік жазбаны рұқсатсыз өзгертуден қорғау

Басқару серверінің ішкі пайдаланушы есептік жазбасын рұқсатсыз өзгертуден қорғау үшін қосымша опцияны қосуды ұсынамыз. Бұл қорғаныс әрбір ішкі пайдаланушы үшін бөлек конфигурациялануы керек.

Басқару сервері бар құрылғы үшін бөлек басқару тобы

Басқару сервері үшін бөлінген басқару тобын жасау ұсынылады. Бұл топқа арнайы кіру құқықтарын беріңіз және ол үшін қауіпсіздік саясатын жасаңыз.

Басқару серверінің қорғау деңгейін әдейі төмендетпеу үшін осы басқару тобын басқара алатын есептік жазбалар тізімін шектеу ұсынылады.

KLAdmins және KLOperators топтары

KLAdmins және KLOperators пайдаланушы топтары Kaspersky Security Center орнату кезінде автоматты түрде жасалады. KLAdmins тобына барлық құқықтар ұсынылған. KLOperators тобына Оқу және Орындау құқықтары ұсынылған. KLAdmins тобына берілген құқықтар жиынтығы **өзгертуге келмейді**.

Стандартты операциялық жүйені басқару құралдарын пайдалану арқылы KLAdmins және KLOperators топтарын қарап шығуға және осы топтардың құрамына өзгертулер енгізуге болады.

Басқару серверімен жұмыс істеуге арналған ережелерді әзірлеу кезінде ақпараттық қауіпсіздік маманына штаттық тапсырмаларды орындау үшін толық қатынас (және KLAdmins тобына қосылу) қажет болады ма екенін анықтау қажет.

Негізгі басқару тапсырмаларының көпшілігі ұйымдағы бөлімшелер (немесе бір бөлімшенің әртүрлі қызметкерлері) арасында және нәтижесінде, әртүрлі есептік жазбалар арасында бөлінуі мүмкін. Сондай-ақ, Kaspersky Security Center бағдарламасында басқару топтарына қатынасу бойынша шектеу қойылуы мүмкін. Нәтижесінде, KLAdmins тобындағы есептік жазбалар бойынша авторизация стандартты емес жүріс-тұрыс болатын пайдалану үлгісін іске асыра аласыз, бұл инцидент ретінде қарастырылуы мүмкін.

Егер Kaspersky Security Center жүйелік есептік жазба астында орнатылған болса, топтар тек Басқару сервері бар құрылғыда жасалады. Бұл жағдайда топқа Kaspersky Security Center орнату кезінде жасалған есептік жазбалардың ғана қосылғанына көз жеткізуді ұсынамыз. Kaspersky Security Center орнату кезінде автоматты түрде жасалған KLAdmins тобына басқа пайдаланушы топтарын (жергілікті және/немесе домендік) қосу ұсынылмайды. Сондай-ақ, бұл топты өзгерту құқықтарын шектеу керек. KLAdmins тобы артықшылықсыз дара есептік жазбаларды қамтуы керек.

Орнату доменге енгізілген пайдаланушы есептік жазбасы астында орындалса, KLAdmins және KLOperators топтары Басқару серверінде де, Басқару сервері кіретін доменде де жасалады. Жүйе есептік жазбасының астында орнату жағдайында сияқты тәсілді пайдалану ұсынылады.

"Бас әкімші" рөліндегі мүшелікті шектеу

Пайдаланушылардың мүшелігін "Бас әкімші" рөлімен шектеу ұсынылады.

Әдепкі бойынша, Басқару серверін орнатқаннан кейін "Бас әкімші" рөлі жергілікті құрылғы әкімшілері тобына және құрылған KLAdmins тобына тағайындалады. Бұл басқару үшін ыңғайлы, бірақ қауіпсіздік тұрғысынан өте маңызды, өйткені "Бас әкімші" рөлі артықшылықтардың өте кең ауқымына ие – бұл рөлді пайдаланушыларға тағайындау қатаң түрде реттелуі керек.

Жергілікті әкімшілерді Kaspersky Security Center әкімшісінің құқықтары бар пайдаланушылар тізімінен алып тастауға болады. "Бас әкімші" рөлін KLAdmins тобынан жою мүмкін емес. Оған Басқару серверін басқару үшін пайдаланылатын KLAdmins тобының есептік жазбаларын қосуға болады.

Домендік түпнұсқалық растама пайдаланылса, Kaspersky Security Center жүйесінде домен әкімшілері есептік жазбаларының артықшылықтарын шектеу ұсынылады. Әдепкі бойынша, бұл есептік жазбаларға "Бас әкімші" рөлі тағайындалады. Сондай-ақ, домен әкімшісі "Бас әкімші" рөлін алу үшін өз тіркелгісін KLAdmins тобына қоса алады. Бұған жол бермеу үшін, Kaspersky Security Center қауіпсіздік параметрлеріне "Домен әкімшілері" ("Domain Admins") тобын қосып, ол үшін тыйым салу ережелерін анықтауға болады. Бұл ережелер рұқсат ететіндерден басым болады.

Сондай-ақ, бұрыннан конфигурацияланған құқықтар жиынтығы бар алдын ала анықталған пайдаланушы рөлдерін пайдалануға болады.

Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау

Басқару серверінің әртүрлі функцияларына пайдаланушылар мен пайдаланушы топтары үшін қатынасу құқықтарын икемді конфигурациялау мүмкіндіктерін пайдалану ұсынылады.

Рөлдер негізінде қатынасуды басқару арқасында алдын ала конфигурацияланған құқықтар жиынтығы бар осы типтік пайдаланушы рөлдерін жасауға және пайдаланушыларға олардың қызметтік міндеттеріне қарай рөлдер тағайындауға болады.

Қатынасуды басқарудың рөлдік моделінің негізгі артықшылықтары:

- басқарудың қарапайымдылығы;
- рөлдер иерархиясы;

- ең аз артықшылық қағидаты;
- міндеттерді бөлу.

Сіз кірістірілген рөлдерді пайдалана аласыз және оларды лауазымдар негізінде нақты қызметкерлерге тағайындай аласыз немесе әбден жаңа рөлдерді жасай аласыз.

Рөлдерді конфигурациялау кезінде құрылғыны қорғау күйін өзгертуге және үшінші тарап бағдарламалық жасақтамасын қашықтан орнатуға қатысты артықшылықтарға ерекше назар аударыңыз:

- Басқару топтарын басқару.
- Басқару серверіне қатысты әрекеттер.
- Қашықтан орнату.
- Оқиғаларды сақтау және хабарландыруларды жіберу параметрлерін өзгерту.

  Бұл артықшылық, оқиға орын алған кезде Басқару сервері бар құрылғыда скриптті немесе орындалатын модульді іске қосатын хабарландыруларды конфигурациялауға мүмкіндік береді.

Қолданбаларды қашықтан орнату үшін бөлек есептік жазба

Қатынасу құқықтарын негізгі шектеуден басқа, барлық есептік жазбалар үшін ("Бас әкімші" немесе басқа мамандандырылған есептік жазбадан басқа) қолданбаларды қашықтан орнату мүмкіндігін шектеу ұсынылады.

Қолданбаларды қашықтан орнату үшін бөлек есептік жазбаны пайдалану ұсынылады. Бөлек есептік жазбаға рөл немесе рұқсаттар тағайындауға болады.

Windows артықшылықты қатынасы қауіпсіздігін қамтамасыз ету

Артықшылықты қатынасудың қауіпсіздігін қамтамасыз ету бойынша Microsoft ұсыныстарын қарап шығуды ұсынамыз. Осы ұсыныстарды қарап шығу үшін Артықшылықты қатынасудың қауіпсіздігін қамтамасыз ету бөліміне өтіңіз.

Негізгі ұсыныстардың бірі – артықшылықты қатынасы бар жұмыс станцияларын (PAW) орналастыру болып табылады.

Қызметтердің басқарылатын есептік жазбаларын (MSA) және қызметтердің топтық басқарылатын есептік жазбаларын (gMSA) Басқару сервері қызметтерін іске қосу үшін пайдалану

Active Directory ішінде MSA/gMSA қызметтерін қауіпсіз іске қосу үшін есептік жазбалардың арнайы түрі бар. Kaspersky Security Center бағдарламасы қызметтің басқарылатын есептік жазбаларын (MSA) және қызметтің топтық басқарылатын есептік жазбаларын (gMSA) қолдайды. Доменіңізде осындай есептік жазбалар қолданылса, олардың біреуін Басқару сервері қызметі үшін есептік жазба ретінде таңдай аласыз.

Барлық пайдаланушы мен пайдаланушы әрекеттерінің тұрақты аудиті

Басқару сервері орнатылған құрылғыдағы барлық пайдаланушылардың тұрақты аудитін жүргізу ұсынылады. Бұл, құрылғының ықтимал бұзылуымен байланысты қауіпсіздік қатерлерінің кейбір түрлеріне жауап беруге мүмкіндік береді.

Сондай-ақ басқару серверіне қосу және ажырату, басқару серверіне қатемен қосу және нысандарды өзгерту (тексеруді басқаруға қолдау көрсететін нысандар үшін) сияқты пайдаланушылардың әрекеттерін бақылауға болады.

Басқару серверін қорғауды басқару

Басқару серверін қорғау бағдарламасын таңдау

Басқару сервері орнатылған құрылғыны қорғауға арналған қолданбаны таңдау Басқару серверін орналастыру түріне және жалпы қорғау стратегиясына байланысты.

Басқару серверін бөлінген құрылғыда қолданатын болсаңыз, құрылғыны Басқару серверімен қорғау үшін Kaspersky Endpoint Security бағдарламасын таңдау ұсынылады. Бұл құрылғыны қорғау үшін барлық қолжетімді технологияларды, соның ішінде әрекет талдауы модульдерін пайдалануға мүмкіндік береді.

Басқару сервері инфрақұрылымда бұрыннан бар және бұған дейін басқа тапсырмаларды орындау үшін пайдаланылған құрылғыда орнатылған болса, келесі қорғау қолданбалары ұсынылады:

- Kaspersky Industrial Cyber Security for Nodes. Бұл бағдарламаны өнеркәсіптік желіге кіретін құрылғыларға орнату ұсынылады. Kaspersky Industrial Cyber Security for Nodes – әртүрлі өнеркәсіптік бағдарламалық жасақтама өндірушілерімен үйлесімділік сертификаттары бар бағдарлама.
- Ұсынылатын қауіпсіздік шешімдері. Басқару сервері басқа бағдарламалық жасақтамасы бар құрылғыда орнатылған болса, сіз бағдарламалық жасақтама өндірушісінің антивирустық шешімдерді пайдалану бойынша ұсыныстарын оқып шығуыңыз керек (қорғау бағдарламасын таңдау бойынша ұсыныстар бұрыннан бар болуы мүмкін және сенімді аймақты конфигурациялау қажет болуы мүмкін).

Бағдарламаны қорғау үшін бөлек қауіпсіздік саясатын жасау

Басқару серверінің қорғау қолданбалары үшін бөлек қауіпсіздік саясатын жасау қажет. Бұл саясат клиент құрылғыларының қауіпсіздік саясатынан өзгеше болуы керек. Бұл тәсілдеме басқа құрылғылардың қорғау деңгейіне әсер етпестен, Басқару серверіне барынша сәйкес келетін қауіпсіздік параметрлерін орнатуға мүмкіндік береді.

Басқару сервері бар құрылғыны бөлек басқару тобына тағайындау арқылы құрылғыларды топтарға бөлу ұсынылады, ол үшін арнайы қауіпсіздік саясатын жасауға болады.

Қорғаныс модульдері

Басқару серверімен бір құрылғыда орнатылған үшінші тарап бағдарламалық жасақтамасының өндірушісінен ерекше ұсыныстар болмаса, барлық қолжетімді қорғаныс модульдерін іске қосу және конфигурациялау ұсынылады (олардың жұмысын белгілі бір уақыт аралығында тексергеннен кейін).

Басқару сервері арқылы құрылғының желілік экранын конфигурациялау

Басқару сервері бар құрылғыда желілік экранды әкімшілер Басқару серверіне Басқару консолі немесе Kaspersky Security Center Web Console консолі арқылы қосыла алатын құрылғылардың санын шектейтіндей етіп конфигурациялау ұсынылады.

Әдепкі бойынша Басқару сервері Басқару консоліне қосылу үшін 13291-портты және Kaspersky Security Center Web Console веб консолінe қосылу үшін 13299-портты пайдаланады. Басқару серверін осы порттар арқылы басқаруға болатын құрылғылардың санын шектеу ұсынылады.

Клиент құрылғыларын қорғауды басқару

Орнату пакеттеріне лицензиялық кілттерді қосуды шектеу

Орнату пакеттері, Packages қалтасына салынған Басқару серверінің ортақ қатынас бар қалтасында сақталады. Орнату пакетіне лицензиялық кілттер қосылса, оларды осы ортақ қатынасы бар қалтаға оқу құқығы бар барлық пайдаланушылар оқи алады.

Лицензиялық кілттің бұзылуын болдырмау үшін орнату пакеттеріне лицензиялық кілттерді қоспау ұсынылады.

Лицензиялық кілттерді басқарылатын құрылғыларға автоматты түрде тарату пайдалануды, Басқарылатын бағдарлама үшін лицензиялық кілтті қосу тапсырмасы арқылы орналастыруды, сондай-ақ құрылғыларға белсендіру кодын немесе кілт файлын қолмен қосуды ұсынамыз.

Басқару топтары арасында құрылғыларды автоматты түрде жылжыту ережелері

Басқару топтары арасында құрылғыларды автоматты түрде жылжыту үшін ережелерді пайдалануды шектеу ұсынылады.

Автоматты түрде жылжыту ережелерін пайдалану, құрылғыға жылжытуға дейінгіден көбірек артықшылықтар беретін саясаттар таратуға әкелуі мүмкін.

Клиент құрылғысын басқа басқару тобына жылжыту, оған саясат параметрлерінің таралуына әкелуі мүмкін. Бұл саясат параметрлері қонақ ретіндегі және сенімсіз құрылғыларға тарату үшін қажет болмауы мүмкін.

Бұл ұсыныс құрылғыларды басқару топтары бойынша бастапқы таратуға қолданылмайды.

Тарату нүктелері мен қосылым шлюздері бар құрылғыларға арналған қауіпсіздік талаптары

Желілік агент орнатылған құрылғыларды тарату нүктесі ретінде пайдалануға және келесі функцияларды орындауға болады:

- Басқару серверінен алынған жаңартулар мен орнату пакеттерін топтағы клиент құрылғыларына тарату.
- Клиент құрылғыларында үшінші тарап бағдарламаларын және Kaspersky бағдарламаларын қашықтан орнату.
- Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

Ұйымның желісінде тарату нүктелерін орналастыру мыналар үшін қолданылады:

- Басқару серверіне түсетін жүктемені азайту;
- трафикті оңтайландыру;
- Басқару серверіне желінің жетуі қиын бөліктеріндегі құрылғыларға қатынасу мүмкіндік беру.

Қолжетімді мүмкіндіктерді ескере отырып, рұқсат етілмеген қатынасудың кез келген түрінен тарату нүктелері ретінде әрекет ететін құрылғыларды, соның ішінде физикалық түрде қорғау ұсынылады.

Тарату нүктелерін автоматты түрде тағайындауды шектеу

Басқаруды жеңілдету және желінің жұмыс істеу қабілетін сақтау үшін тарату нүктелерін автоматты түрде тағайындауды пайдалануды ұсынамыз. Дегенмен, өнеркәсіптік және шағын желілерде тарату нүктелерін автоматты түрде тағайындаудан аулақ болу ұсынылады, өйткені тарату нүктелеріне, мысалы, операциялық жүйе құралдарының көмегімен мәжбүрлеп қашықтан орнату тапсырмаларын орындау үшін пайдаланылатын есептік жазбалардың құпия мәліметін беруге болады.

Өнеркәсіптік және шағын желілерде тарату нүктелерін қолмен тағайындауға болады.

Қажет болса, Тарату нүктелерінің әрекетіндегі есепті де қарап шығуға болады.

Kaspersky Security Center пайдаланушыларының құрылғыларына арналған қауіпсіздік талаптары

Kaspersky Security Center пайдаланушыларының құрылғыларына арнайы қауіпсіздік талаптары қолданылуы керек. Бұл құрылғыларды кез келген рұқсатсыз кіруден (соның ішінде физикалық) қорғауды ұсынамыз:

Kaspersky Security Center пайдаланушы құрылғыларына мыналар кіреді:

- Пайдаланушылар Kaspersky Security Center Web Console-ге браузер арқылы қосылатын құрылғылар.
- Пайдаланушылар Kaspersky Security Center-ге MMC негізіндегі басқару консолін пайдалану арқылы қосылатын құрылғылар.
- OpenAPI арқылы басқару серверімен әрекеттесетін қолданбалардан Kaspersky Security Center жүйесіне қосылған құрылғылар.

Kaspersky Security Center Web Console орнатылған құрылғыларға арналған қауіпсіздік талаптары

Kaspersky Security Center Web Console орнатылған құрылғылар Kaspersky Security Center жүйесін басқару үшін пайдаланылады, сондықтан бұл құрылғылардың қауіпсіздігіне арнайы талаптар қолданылуы керек. Бұл құрылғыларды кез келген рұқсатсыз кіруден (соның ішінде физикалық) қорғауды ұсынамыз.

Басқарылатын қолданбалар қорғанысын конфигурациялау

Басқарылатын қолданба саясаттары

Kaspersky Security Center (желілік агент, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent және т.б.) пайдаланылатын қолданбалары мен құрамдастарының әр түрі үшін саясат жасауға кеңес береміз. Бұл топтық саясат барлық басқарылатын құрылғыларға (түбірлік басқару тобына) немесе конфигурацияланған жылжыту ережелеріне сәйкес жаңа басқарылатын құрылғылар автоматты түрде кіретін бөлек топқа қолданылуы керек.

Қорғанысты өшіру және қолданбаны жою үшін құпиясөзді орнату

Қаскүнемдердің Kaspersky қауіпсіздік бағдарламасын өшіруіне жол бермеу үшін қорғанысты өшіру және Kaspersky қауіпсіздік бағдарламасын жою үшін құпиясөз орнатуды ұсынамыз. Құпиясөзді, мысалы, Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Servers, желілік агент және басқа Kaspersky қолданбалары үшін орнатуға болады. Құпиясөзбен қорғауды қосқаннан кейін бұл параметрлерді "құлыппен" жабу арқылы бұғаттау ұсынылады.

Клиенттік құрылғыны Басқару серверге қолмен қосу үшін құпия сөзді көрсету (klmover утилитасы)

klmover утилитасы клиенттік құрылғыны Басқару серверге қолмен қосуға мүмкіндік береді. Желілік агент клиент құрылғысына орнатылған кезде, утилита автоматты түрде Желілік агент орнату қалтасына көшіріледі.

Зиянкестер құрылғыларды Басқару серверіңіздің басқаруынан шығаруына жол бермеу үшін klmover утилитасын іске қосқан кезде құпия сөзбен қорғауды міндетті түрде қосу ұсынылады. Құпиясөз қорғанысын қосу үшін Желілік агент саясаты параметрлерінде **Жою құпиясөзін пайдалану** опциясын таңдаңыз.

klmover утилитасына жергілікті әкімші құқықтары қажет. klmover утилитасын іске қосу үшін құпия сөзді қорғауды жергілікті әкімші құқықтарынсыз жұмыс істейтін құрылғылар үшін орнатпауға болады.

Жою құпиясөзін пайдалану параметрін қосу кезінде Cleaner (cleaner.exe) көмегімен құпиясөзді қорғау да қосылады.

Kaspersky Security Network қолдану

Басқарылатын қолданбалардың барлық саясаттарында және Басқару серверінің сипаттарында Kaspersky Security Network (KSN) пайдалану және ағымдағы KSN мәлімдемесін қабылдау ұсынылады. Басқару серверін жаңарту кезінде сіз жаңартылған KSN мәлімдемесін де қабылдай аласыз. Бұлттық қызметтерді пайдалануға заңнамамен немесе өзге де нормативтік актілермен тыйым салынған жағдайларда, KSN қызметін қоса алмайсыз.

Басқарылатын құрылғыларды жүйелі түрде тексеру

Барлық құрылғылар топтары үшін құрылғыларды толықтай тексеруді кезең-кезең іске қосатын тапсырманы жасау ұсынылады.

Жаңа құрылғыларды табу

Құрылғыны табу параметрлерін дұрыс конфигурациялау: Active Directory интеграциясын орнату және жаңа құрылғыларды табу үшін IP мекенжайлары ауқымдарын көрсету ұсынылады.

Қауіпсіздік мақсатында, сіз барлық жаңа құрылғыларды қамтитын әдепкі бойынша басқару тобын және осы топқа қолданылатын әдепкі бойынша саясаттарды пайдалана аласыз.

Ортақ қатынасы бар қалтаны анықтау

Басқару сервері Windows басқаруымен жұмыс істейтін құрылғыда орналастырылған болса, бұрыннан бар ортақ қатынасы бар қалта таңдалса (мысалы, орнату пакеттерін және жаңартылатын дерекқорларды орналастыру үшін пайдаланылады), оқу рұқсаттары "Барлығы" (Everyone) тобына, ал жазу рұқсаттары KLAdmins тобына берілгенін тексеруді ұсынамыз.

Басқару серверіне техникалық қызмет көрсету

Басқару сервері деректерін сақтық көшірмелеу

Деректердің сақтық көшірмесі Басқару сервері деректерін жоғалтпай қалпына келтіруге мүмкіндік береді.

Әдепкі бойынша, сақтық көшірмелеу тапсырмасы Kaspersky Security Center орнатылғаннан кейін автоматты түрде жасалады және сақтық көшірмелерді тиісті директорияда сақтай отырып, мерзімді түрде орындалады. Пайдаланушы сақтық көшірмелеу тапсырмасының параметрлерін өзгерте алады:

- резервтік көшірмелеу жиілігін арттыру;
- көшірмелерді сақтау үшін ерекше директорияны анықтау;
- сақтық көшірме құпиясөзін өзгерту.

Сақтық көшірмелерді әдепкі бойынша директориядан басқа директориядан сақтаған кезде, осы директорияның ACL шегін шектеу ұсынылады. Басқару серверінің есептік жазбалары мен Басқару серверінің дерекқоры серверінің осы директорияда жазуға қатынасу рұқсаты болуы керек.

Басқару серверіне техникалық қызмет көрсету

Басқару серверіне қызмет көрсету арқасында дерекқор көлемін қысқартуға, бағдарлама жұмысының өнімділігі мен сенімділігін арттыруға болады. Басқару серверіне аптасына бір реттен сиретпей техникалық қызмет көрсету ұсынылады.

Басқару серверіне техникалық қызмет көрсету тиісті тапсырманың көмегімен орындалады. Басқару серверіне техникалық қызмет көрсету барысында бағдарлама келесі әрекеттерді орындайды:

- дерекқорды қателердің болуы тұрғысынан тексереді;
- дерекқордың индекстерін қайта құрады;
- дерекқордың статистикасын жаңартады;
- дерекқорды қысады (қажет болса).

Басқару сервері бар құрылғыдағы операциялық жүйені және үшінші тарап бағдарламалық жасақтамасын жаңарту

Басқару сервері бар құрылғыда операциялық жүйе мен үшінші тарап бағдарламалық жасақтамасының жаңартуларын жүйелі түрде орнату ұсынылады.

Клиент құрылғыларына Басқару серверіне тұрақты қосылым қажет емес, сондықтан жаңартуларды орнатқаннан кейін құрылғыны Басқару серверімен қауіпсіз қайта жүктеуге болады. Басқару сервері әрекетсіз тұрғанда клиент құрылғыларында тіркелген барлық оқиғалар, қосылым қалпына келтірілгеннен кейін оған жіберіледі.

Оқиғаларды үшінші тарап жүйелеріне беру

Бақылау және есеп беру

Қауіпсіздік мәселелеріне дер кезінде жауап беру үшін бақылау және есеп беру функцияларын конфигурациялауға болады.

Оқиғаларды SIEM жүйелеріне экспорттау

Елеулі нұқсан келтірілмей тұрып, мәселелерді мүмкіндігінше тез анықтау үшін оқиғаларды SIEM жүйесіне жіберуді пайдалану ұсынылады.

Аудит оқиғалары туралы электрондық пошта арқылы хабарландыру

Kaspersky Security Center бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Орын алған төтенше жағдайларға дер кезінде жауап беру үшін Басқару серверін ол жариялайтын аудит оқиғалары, критикалық оқиғалар, функционалдық ақаулар және ескертулер туралы хабарландыруларды жіберуге конфигурациялау ұсынылады.

Аудит оқиғалары жүйеішілік болғандықтан, олар сирек тіркеледі және мұндай оқиғалар туралы хабарландырулардың саны пошта жіберілімі үшін әбден қолайлы.

Басқару серверінің жұмысы туралы статистикалық ақпарат

Қауіпсіздік мәселелеріне жедел жауап беру үшін Simple Network Management Protocol (SNMP) арқылы үшінші тарап қолданбаларына басқару серверінің жұмысы туралы статистикалық ақпаратты жіберуді реттеу ұсынылады.

Үшінші тарап ақпараттық жүйелерінің қауіпсіздігі бойынша ұсыныстар

CIS Benchmarks қауіпсіздік бойынша ұсыныстары

Басқару сервері және Желілік агент қолдайтын операциялық жүйелердің, виртуализация платформаларының немесе дерекқор серверлерінің нұсқаларын пайдаланған кезде, бұл ақпараттық жүйелерді дәл конфигурациялау үшін Center for Internet Security (CIS) ақпаратты қорғау әдістерін, егер олар бар болса, пайдалану ұсынылады.

Center for Internet Security (CIS) – ақпараттық технологиялар саласындағы қауіпсіздікті арттырумен айналысатын коммерциялық емес ұйым. Атап айтқанда, CIS ұйымы CIS Controls және CIS Benchmarks сияқты қауіпсіздік стандарттарын әзірлейді және таратады. Бұл стандарттар ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету бойынша ұсыныстар мен тәжірибелердің жиынтығы болып табылады.

CIS МД порталында Басқару сервері және Желілік агент қолдау көрсететін келесі ақпараттық жүйелердің нұсқалары үшін ұсыныстар бар:

- Келесі отбасылардың операциялық жүйелері:
  - Жұмыс станцияларына арналған Windows
  - Серверлерге арналған Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware виртуализация платформалары
- Дерекқор серверлері:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Astra Linux операциялық жүйесі үшін қауіпсіздік ұсыныстары

Astra Linux операциялық жүйесін пайдаланған кезде Astra Linux сәйкес нұсқасы үшін Red Book атты кітапта сипатталған қауіпсіздік ұсыныстарын ұстану керек.

РЕД ОС операциялық жүйесі үшін қауіпсіздік ұсыныстары

RED OS операциялық жүйесін пайдаланған кезде, RED OS ресми құжаттамасында сипатталған әкімші нұсқаулығындағы қауіпсіздік ұсыныстарын орындау керек.

Kaspersky қауіпсіздік қолданбаларын пайдалануға қатысты ұсыныстар

Kaspersky Endpoint Security for Windows бағдарламасында KLAdmin құпиясөзін пайдалану

Kaspersky Endpoint Security for Windows орнатылған құрылғыны компьютерлік сауаттылығы әртүрлі деңгейдегі бірнеше пайдаланушы қолдана алады. Пайдаланушылардың Kaspersky Endpoint Security for Windows қолданбасына және оның параметрлеріне шектеусіз кіру мүмкіндігі болса, құрылғыны қорғаудың жалпы деңгейі төмендеуі мүмкін. Құпиясөзбен қорғау мүмкіндігі пайдаланушыларға берілген құқықтарға (мысалы, қолданбаны өшіру рұқсаты) сәйкес олардың Kaspersky Endpoint Security for Windows жүйесіне кіруін шектеуге мүмкіндік береді.

Kaspersky Endpoint Security for Windows қолданбасына және оның параметрлеріне кіруді шектеудің бір жолы — KLAdmin есептік жазбасын пайдалану. KLAdmin есептік жазбасы — Kaspersky Endpoint Security for Windows қолданбасына шексіз кіру рұқсаты бар әкімші есептік жазбасы. KLAdmin есептік жазбасы Kaspersky Endpoint Security for Windows қолданбасында құпиясөзбен қорғалған кез келген әрекетті орындауға құқылы. KLAdmin есептік жазбасының құқықтарын қайтарып алу мүмкін емес. KLAdmin есептік жазбасы үшін құпиясөзді Kaspersky Endpoint Security for Windows саясат сипаттарында орнатуға болады. Kaspersky Endpoint Security for Windows әкімшісі KLAdmin есептік жазбасына арналған құпиясөзді қауіпсіз пайдалануға толықтай жауапты. Ұйымыңыздың жеке құпиясөз саясаты болса, сол саясаттағы нұсқауларды орындаңыз.

Ұйымыңызды KLAdmin құпиясөзін ұрлаудан қорғау үшін мына қадамдарды орындаңыз:

- **Жалпы талаптар.**

  Есептік жазба атын немесе атының бір бөлігін құпиясөз ретінде пайдаланбаңыз.

- **Құпиясөздің минималды ұзындығына қойылатын талаптар.**

  Кемінде 10 таңбадан тұратын құпиясөз жасаңыз.

- **Бірнеше таңба түрін пайдалану талаптары.**

  Әртүрлі санаттағы таңбаларды қамтитын күрделі құпиясөз орнатыңыз: кіші және бас әріптер, сандар және арнайы таңбалар.

- **Құпиясөздің жарамдылық мерзіміне қойылатын талаптар.**

  Құпиясөздің минималды жарамдылық мерзімін 90 күнге орнатыңыз. Жаңа құпиясөз соңғы 24 құпиясөздің ешқайсысымен бірдей болмауы керек.

Орналастыруға дайындық

Бұл бөлімде Kaspersky Security Center орналастырудың алдында орындау қажет қадамдар сипатталған.

Kaspersky Security Center орналастыруды жоспарлау

Бұл бөлім келесі өлшемшарттарға байланысты ұйымның желісінде Kaspersky Security Center құрамдастарын орналастырудың оңтайлы нұсқалары туралы ақпаратты қамтиды:

- Құрылғылардың жалпы санын
- Ұйымдық немесе географиялық оқшауланған бөлімшелердің (кеңселер, филиалдар) болуы
- Тар арналармен байланған оқшауланған желілердің болуы
- Интернеттен Басқару серверіне қатынасу қажеттілігі

Қорғаныс жүйесін орналастырудың типтік тәсілдері

Бұл бөлімде Kaspersky Security Center көмегімен ұйымның желісінде қорғаныс жүйесін орналастырудың типтік тәсілдері сипатталған.

Жүйені барлық түрлердің рұқсатсыз қатынасуынан қорғауды қамтамасыз ету қажет. Бағдарламаны құрылғыға орнатпас бұрын, операциялық жүйеге арналған барлық қолжетімді қауіпсіздік жаңартуларын орнатып, Басқару серверлері мен тарату нүктелерін физикалық қорғауды қамтамасыз ету ұсынылады.

Келесі орналастыру схемаларын қолдана отырып, Kaspersky Security Center көмегімен ұйымның желісінде қорғаныс жүйесін орналастыруға болады:

- Kaspersky Security Center құралдарымен қорғау жүйесін келесі тәсілдердің бірімен орналастыру:
  - Басқару консолі арқылы;
  - Kaspersky Security Center Web Console арқылы.

  Kaspersky бағдарламаларын клиент құрылғыларына орнату және клиент құрылғыларын Басқару серверіне қосу Kaspersky Security Center көмегімен автоматты түрде жүзеге асырылады.

  Орналастырудың негізгі схемасы, Басқару консолі арқылы қорғаныс жүйесін орналастыру. Kaspersky Security Center Web Console пайдалану браузер арқылы Kaspersky бағдарламаларын орнатуға мүмкіндік береді.

- Kaspersky Security Center бағдарламасында құрылған жеке орнату пакеттері арқылы қорғаныс жүйесін қолмен орналастыру.

  Kaspersky бағдарламаларын клиент құрылғыларына және әкімшінің жұмыс станциясына орнату қолмен жүргізіледі, клиент құрылғыларын Басқару серверіне қосу параметрлері Желілік агентті орнату кезінде белгіленеді.

  Бұл орналастыру нұсқасын қашықтан орнату мүмкін болмаған жағдайда қолдану ұсынылады.

Kaspersky Security Center бағдарламасы Active Directory топтық саясаттары арқылы қорғаныс жүйесін орналастыруға да мүмкіндік береді.

Kaspersky Security Center бағдарламасын ұйымның желісінде орналастыруды жоспарлау туралы

Бір Басқару сервері 100 000-нан аспайтын құрылғыларға қызмет көрсете алады. Егер ұйымның желісіндегі құрылғылардың жалпы саны 100 000-нан асса, орталықтандырылған басқаруды жеңілдету үшін иерархияға біріктірілген бірнеше Басқару серверлерін ұйымның желісіне орналастыру керек.

Егер ұйымның құрамында өз әкімшілері бар үлкен географиялық қашықтағы кеңселер (филиалдар) болса, осы кеңселерде Басқару серверлерін орналастырған жөн. Әйтпесе, мұндай кеңселерді тар арналармен байланысқан оқшауланған желілер ретінде қарастыру керек, "Типтік конфигурация: өзіндік әкімшілері бар бірнеше ірі кеңселер" бөлімін қараңыз.

Егер тар арналармен байланысқан оқшауланған желілер болса, мұндай желілердегі трафикті үнемдеу үшін бір немесе бірнеше Желілік агентті тарату нүктелері етіп тағайындау керек (тарату нүктелерінің санын есептеу үшін кестені қараңыз). Бұл жағдайда, оқшауланған желінің барлық құрылғылары осындай "жергілікті жаңарту орталықтарынан" жаңартулар алады. Тарату нүктелері Басқару серверінен (әдепкі жүріс-тұрыс) және интернет орналастырылған Kaspersky серверлерінен жаңартуларды жүктеп ала алады, "Типтік конфигурация: көптеген шағын оқшауланған кеңселер" бөлімін қараңыз.

"Kaspersky Security Center типтік конфигурациялары" бөлімінде Kaspersky Security Center типтік конфигурацияларының егжей-тегжейлі сипаттамасы берілген. Орналастыруды жоспарлау кезінде, ұйымның құрылымына байланысты, ең қолайлы типтік конфигурацияны таңдау керек.

Орналастыруды жоспарлау кезеңінде Басқару серверіне X.509 арнайы сертификатын белгілеу қажеттілігін ескеру қажет. Басқару серверіне X.509 арнайы сертификатын белгілеу келесі жағдайларда орынды болуы мүмкін (толық емес тізім):

- SSL трафигін SSL termination proxy арқылы инспекциялау үшін немесе Reverse Proxy қолдану үшін;
- ұйымның жалпыға ортақ кілті (PKI) инфрақұрылымымен біріктіру үшін;
- сертификат өрістерінің қажетті мәндерін белгілеу үшін;
- сертификаттың қажетті криптографиялық беріктігін қамтамасыз ету үшін.

Ұйымның қорғаныс құрылымын таңдау

Ұйымның қорғаныс құрылымын таңдау келесі факторларды анықтайды:

- Ұйым желісінің топологиясы.
- Ұйымдық құрылым.
- Желіні қорғауға жауапты қызметкерлердің саны және олардың арасындағы міндеттерді бөлу.
- Қорғанысты басқару құрамдастарын орнатуға бөлінуі мүмкін аппараттық ресурстар.
- Ұйымның желісіндегі қорғаныс құрамдастарының жұмысына бөлінуі мүмкін байланыс арналарының өткізу қабілеті.
- Ұйым желісіндегі маңызды басқару операцияларын орындаудың рұқсат етілген уақыты. Маңызды басқару операцияларына, мысалы, антивирустық дерекқордың жаңартуларын тарату және клиент құрылғыларына арналған саясатты өзгерту кіреді.

Қорғаныс құрылымын таңдағанда, алдымен орталықтандырылған қорғаныс жүйесін басқаруға болатын қолжетімді желілік және аппараттық ресурстарды анықтау ұсынылады.

Желілік және аппараттық инфрақұрылымды талдау үшін келесі әрекеттер тәртібі ұсынылады:

1. Қорғаныс орналастырылатын желінің келесі параметрлерін анықтау:
   - желі сегменттері саны;
   - желінің жеке сегменттері арасындағы байланыс арналарының жылдамдығы;
   - желі сегменттерінің әрқайсысында басқарылатын құрылғылар саны;
   - қорғаныстың жұмыс істеуі үшін бөлінуі мүмкін әрбір байланыс арнасының өткізу қабілеттілігі.
2. Барлық басқарылатын құрылғылар үшін өзекті басқару операцияларының рұқсат етілген орындалу уақытын анықтау.
3. 1 және 2 тармақтарындағы ақпаратты, сондай-ақ басқару серверін жүктемелік тестілеу деректерін талдау. Жүргізілген талдау негізінде келесі сұрақтарға жауап беріңіз:
   - Барлық клиенттерге бір Басқару серверімен қызмет көрсету мүмкін бе немесе Басқару серверлері иерархиясы қажет пе?
   - 2-тармақта анықталған уақыт ішінде барлық клиенттерге қызмет көрсету үшін Басқару серверінің қандай аппараттық конфигурациясы қажет?
   - Байланыс арналарына түсетін жүктемені азайту үшін тарату нүктелерін пайдалану қажет пе?

Аталған сұрақтарға жауап бергеннен кейін, сіз ұйымның рұқсат етілген қорғаныс құрылымдарының жиынтығын жасай аласыз.

Ұйымның желісінде келесі типтік қорғаныс құрылымдарының бірін пайдалануға болады:

- Бір Басқару сервері. Барлық клиент құрылғылары бір Басқару серверіне қосылған. Тарату нүктесінің рөлін Басқару сервері атқарады.
- Тарату нүктелері бар бір Басқару сервері. Барлық клиент құрылғылары бір Басқару серверіне қосылған. Желіде тарату нүктелерінің рөлін атқаратын клиент құрылғылары көрсетілген.
- Басқару серверлерінің иерархиясы. Желінің әрбір сегменті үшін Басқару серверінің жалпы иерархиясына қосылған бөлек Басқару сервері бөлектелген. Тарату нүктесінің рөлін негізгі Басқару сервері атқарады.
- Тарату нүктелері бар Басқару серверлерінің иерархиясы. Желінің әрбір сегменті үшін Басқару серверінің жалпы иерархиясына қосылған бөлек Басқару сервері бөлектелген. Желіде тарату нүктелерінің рөлін атқаратын клиент құрылғылары көрсетілген.

Kaspersky Security Center типтік конфигурациялары

Бұл бөлімде ұйымның желісінде Kaspersky Security Center құрамдастарын орналастырудың келесі типтік конфигурациялары сипатталған:

- Бір кеңсе
- Өзіндік әкімшілері бар бірнеше ірі географиялық бөлінген кеңселер
- Көптеген шағын географиялық бөлінген кеңселер

Типтік конфигурация: бір кеңсе

Ұйымның желісінде бір немесе бірнеше Басқару сервері орналастырылуы мүмкін. Серверлер саны қолжетімді аппараттық жасақтаманың болуына байланысты, сондай-ақ басқарылатын құрылғылардың жалпы санына байланысты таңдалуы мүмкін.

Бір Басқару сервері 100 000-ға дейінгі құрылғыларға қызмет көрсете алады. Таяу болашақта басқарылатын құрылғылардың санын көбейту мүмкіндігін ескеру қажет: бір Басқару серверіне біршама аз құрылғыларды қосу қажет болуы мүмкін.

Басқару серверлері ішкі желіде де, демилитаризацияланған аймақта да орналастырылуы мүмкін, бұл интернеттен Басқару серверлеріне қатынасу қажет пе екендігіне байланысты.

Егер бірнеше Сервер болса, оларды иерархияға біріктіру ұсынылады. Басқару серверлерінің иерархиясының болуы саясат пен тапсырмалардың қайталануын болдырмауға, барлық басқарылатын құрылғылардың көпшілігімен олардың барлығы бір Басқару серверімен басқарылатындай жұмыс істеуге (яғни құрылғыларды іздеуге, құрылғы таңдауларын жасауға, есептер жасауға) мүмкіндік береді.

Типтік конфигурация: өзіндік әкімшілері бар бірнеше үлкен кеңсе

Бірнеше ірі қашықтағы кеңсе болған кезде, әр кеңседе Басқару серверлерін орналастыру мүмкіндігі туралы ойлану керек. Клиент құрылғыларының санына және қолжетімді аппараттық жасақтамаға байланысты әр кеңседе бір немесе бірнеше Басқару серверінен. Бұл жағдайда, кеңселердің әрбірі "Типтік конфигурация: бір кеңсе" ретінде қарастырылуы мүмкін. Басқаруды жеңілдету үшін барлық Басқару серверлері иерархияға, бәлкім, көп деңгейлі иерархияға біріктірілуі керек.

Егер кеңселер арасында құрылғылармен (ноутбуктермен) бірге орын ауыстыратын қызметкерлер болса, Желілік агент саясатында Желілік агентті қосу профильдері жасалуы керек. Желілік агентті қосу профильдері тек Windows және macOS операциялық жүйелері бар құрылғыларды қолдайды.

Типтік конфигурация: қашықтағы көптеген шағын кеңселер

Бұл типтік конфигурация бір бас кеңсені және интернет арқылы бас кеңсеге хабарласа алатын көптеген шағын қашықтағы кеңселерді ұсынады. Қашықтағы кеңселердің әрқайсысы Network Address Translation (бұдан әрі - NAT) артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес, кеңселер бір-бірінен оқшауланған.

Бас кеңседе Басқару серверін орналастыру керек, ал қалған кеңселерде бір немесе бірнеше тарату нүктесін тағайындау керек. Кеңселер арасындағы байланыс интернет арқылы жүзеге асырылатындықтан, тарату нүктелері үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын, тарату нүктелері жаңартуларды Басқару серверінен емес, тікелей Kaspersky серверлерінен, жергілікті немесе желілік қалталардан жүктеп алатындай етіп жасаған жөн.

Егер қашықтағы кеңседе құрылғылардың бір бөлігі Басқару серверіне тікелей қатынаса алмаса (мысалы, Басқару серверіне интернет арқылы қатынасады, бірақ интернетке құрылғылардың барлығы бірдей қатынаса алмайды), онда тарату нүктелерін шлюз режиміне ауыстыру керек. Бұл жағдайда, қашықтағы кеңседегі құрылғылардағы Желілік агенттер Басқару серверіне тікелей емес, шлюз арқылы қосылады (синхрондау мақсатында).

Көп жағдайда басқару сервері қашықтағы кеңседегі желіге сауалнама жүргізе алмайтындықтан, бұл функцияны орындауды тарату нүктелерінің біріне жүктеген жөн.

Басқару сервері қашықтағы кеңседе NAT артында орналасқан басқарылатын құрылғыларға 15000 UDP портына хабарландыру жібере алмайды. Бұл мәселені шешу үшін тарату нүктелері болып табылатын құрылғылардың сипаттарында Басқару серверіне тұрақты қосылым режимін қосуға болады (**Басқару серверімен байланысты үзбеу** жалаушасы). Егер тарату нүктелерінің жалпы саны 300-ден аспаса, бұл режим қолжетімді болады. Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін push серверлерін пайдаланыңыз. Қосымша ақпарат алу үшін келесі бөлімдерді қараңыз: Тарату нүктесін хабарлаушы сервер ретінде қолдану.

Басқару сервері үшін ДҚБЖ таңдау

Басқару сервері пайдаланатын ДҚБЖ таңдау кезінде Басқару сервері қызмет көрсететін құрылғылардың санын басшылыққа алу керек.

Төмендегі кестеде ДҚБЖ рұқсат етілген нұсқалары және оларды ұсынымдары мен қолдану шектеулері аталған.

ДҚБЖ ұсынымдар және шектеулер

ДҚБЖ	Ұсынымдар және шектеулер
SQL Server Express Edition 2016 және одан жоғары	10 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Дерекқордың толып кетуіне жол бермеу үшін оқиғалар қоймасындағы оқиғалардың ең көп санын шектей аласыз. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу. SQL Server Express Edition ДҚБЖ Басқару серверімен және қандай да бір басқа бағдарламамен бірге қолдануға болмайды. Microsoft SQL Express дерекқорына **Windows Update жаңартуларын синхрондау** тапсырмасы үшін қолдау көрсетілмейді.
Express, 2016 және одан жоғары нұсқасынан ерекшеленетін жергілікті SQL Server Edition	Шектеулер жоқ.
Express, 2016 және одан жоғары нұсқалардан ерекшенелетін қашықтағы SQL Server Edition	Егер екі құрылғы бір Windows доменінде болса ғана рұқсат етіледі; егер домендер әртүрлі болса, онда олардың арасында екі жақты сенім қатынасы орнатылуы тиіс.
Жергілікті немесе қашықтағы MySQL 5.5, 5.6 немесе 5.7 (MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 және 5.5.5 нұсқаларына қолдау көрсетілмейді)	10 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.
Жергілікті немесе қашықтағы MySQL 8.0.20 немесе одан жоғары	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.

ДҚБЖ	Ұсынымдар және шектеулер
Жергілікті немесе қашықтағы MariaDB нұсқасы (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.
PostgreSQL, Postgres Pro (қолдау көрсетілетін нұсқаларды қараңыз)	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ жүйелерінің бірін пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.

Егер сіз MSSQL 2019 нұсқасын таңдасаңыз, CU12 немесе одан кейінгі жинақталған патчын пайдалануыңыз керек. Бұл сізге орын алуы мүмкін қателер мен жүйенің шамадан тыс жүктелуін болдырмауға мүмкіндік береді.

SQL Server 2019 бағдарламасын ДҚБЖ ретінде пайдаланған кезде CU12 жинақталған патчын қолдану

SQL Server 2019 бағдарламасын ДҚБЖ ретінде пайдалану кезінде "Бұл сұрауды орындау үшін 'internal' ішкі ресурс пулында жүйелік жад жеткіліксіз" сияқты қателерді болдырмау үшін, CU12 немесе одан кейінгі жинақталған патчты (CU) орнату қажет.

Kaspersky Security Center орнатқаннан кейін келесі қадамдарды орындаңыз:

1. SQL Management Studio көмегімен SQL серверіне қосылыңыз.
2. Келесі пәрменді орындаңыз (егер дерекқор үшін басқа атауды таңдасаңыз, KAV орнына осы атауды қолданыңыз):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. SQL Server 2019 қызметін қайта іске қосыңыз.

Kaspersky Security Center 15.1 нұсқасымен жұмыс істеу үшін MariaDB x64 серверінің конфигурациясы

MariaDB x64 серверін Kaspersky Security Center-мен жұмыс істеу мақсатында сәтті конфигурациялау үшін осы мақалада көрсетілген сервер параметрлерін қоспағанда, әдепкі сервер параметрлерін пайдалану керек.

Kaspersky Security Center 15.1 бағдарламасы MariaDB ДҚБЖ-не қолдау көрсетеді. MariaDB қолдау көрсетілетін нұсқалары туралы қосымша ақпаратты Аппараттық және бағдарламалық талаптар бөлімінен қараңыз.

Kaspersky Security Center үшін MariaDB ДҚБЖ қолдансаңыз, InnoDB және MEMORY қоймасы қолдауын, сондай-ақ UTF-8 және UCS-2 кодтамасы қолдауын қосыңыз.

my.ini файлы үшін ұсынылатын параметрлер

my.ini файлын конфигурациялау үшін:

1. Мәтіндік редактор көмегімен my.ini файлын ашыңыз.

2. my.ini файлының `[mysqld]` бөліміне келесі жолдарды қосыңыз:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< нақты мәні KAV дерекқорының күтілетін өлшемінің 80%-ынан кем болмауы керек >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`innodb_buffer_pool_size` мәні KAV дерекқорының күтілетін өлшемінің 80 пайызынан кем болмауы тиіс. Сервер іске қосылғанда көрсетілген жадтың бөлінетінің ескеріңіз. Егер дерекқор өлшемі көрсетілген буфер өлшемінен аз болса, тек қажетті жад бөлінеді. MariaDB 10.4.3 немесе одан бұрынғы нұсқасын пайдалансаңыз, нақты бөлінген жад көрсетілген буфер өлшемінен шамамен 10 пайызға үлкен.

`innodb_flush_log_at_trx_commit=0` параметрінің мәнін қолдану ұсынылады, себебі "1" немесе "2" мәндері MariaDB жұмыс жылдамдығына теріс әсерін тигізеді. `innodb_file_per_table` параметрінің `1` мәніне орнатылғанын тексеріңіз.

MariaDB 10.1 үшін [mysqld] бөліміне қосымша ретінде келесі жолақтарды енгізіңіз:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

MariaDB 10.6 үшін [mysqld] бөліміне қосымша ретінде келесі жолақтарды енгізіңіз:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Әдепкі бойынша оптимизатордың `join_cache_incremental`, `join_cache_hashed` және `join_cache_bka` конфигурациялары қосулы. Егер бұл баптаулар қосылмаған болса, оларды қосу керек.

Оптимизатор баптауларының қосулы ма екенін тексеру үшін:

1. MariaDB клиент консолінде келесі пәрменді іске қосыңыз:

```
SELECT @@optimizer_switch;
```

2. Шықпасы келесі жолдарды қамтитынына көз жеткізіңіз:

```
join_cache_incremental=on
```

```
join_cache_hashed=on
join_cache_bka=on
```

Бұл жолдар бар болып, on мәнін қамтыса, онда оптимизатор баптаулары қосулы.

Бұл жолдар жоқ болса немесе off мәніне ие болса, келесі әрекеттерді орындаңыз:

1. Мәтіндік редактор көмегімен my.ini файлын ашыңыз.

2. my.ini файлының [mysqld] бөліміне келесі жолдарды қосыңыз:
```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

join_cache_incremental, join_cache_hash және join_cache_bka баптаулары қосулы.

Kaspersky Security Center 15.1 нұсқасымен жұмыс істеу үшін MySQL x64 серверінің конфигурациясы

MySQL x64 серверін Kaspersky Security Center-мен пайдалану мақсатында сәтті конфигурациялау үшін осы мақалада көрсетілген сервер параметрлерін қоспағанда, әдепкі сервер параметрлерін пайдалану керек.

Kaspersky Security Center үшін MySQL ДҚБЖ қолдансаңыз, InnoDB және MEMORY қоймасы қолдауын, сондай-ақ UTF-8 және UCS-2 кодтамасы қолдауын қосыңыз.

my.ini файлы үшін ұсынылатын параметрлер

my.ini файлын конфигурациялау үшін:

1. Мәтіндік редактор көмегімен my.ini файлын ашыңыз.

2. my.ini файлының [mysqld] бөліміне келесі жолдарды қосыңыз:
```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< нақты мәні KAV дерекқорының күтілетін өлшемінің 80%-ынан
кем болмауы керек >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (көп жағдайда сервер шағын транзакцияларды
пайдаланады)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

innodb_buffer_pool_size ішінде көрсетілген жад сервер іске қосылғанда бөлінетін ескеріңіз. Егер дерекқор өлшемі көрсетілген буфер өлшемінен аз болса, тек қажетті жад бөлінеді. Бөлінген жадтың нақты өлшемі көрсетілген буфер өлшемінен шамамен 10 пайызға үлкен. Қосымша ақпарат алу үшін MySQL құжаттамасын қараңыз.

`innodb_flush_log_at_trx_commit = 0` параметрінің мәнін қолдану ұсынылады, себебі "1" немесе "2" мәндері MySQL жұмыс жылдамдығына теріс әсерін тигізеді. `innodb_file_per_table` параметрінің `1` мәніне орнатылғанын тексеріңіз.

Kaspersky Security Center 15.1 бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау

Kaspersky Security Center жүйесімен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін сәтті конфигурациялау үшін осы мақалада көрсетілген сервер параметрлерін қоспағанда, әдепкі сервер параметрлерін пайдалану керек.

Kaspersky Security Center 15.1 бағдарламасы PostgreSQL және Postgres Pro ДҚБЖ қолдайды. Егер сіз осы ДҚБЖ-нің біреуін қолдансаңыз, ДҚБЖ жүйесі мен Kaspersky Security Center бағдарламасының жұмысын оңтайландыру үшін ДҚБЖ серверінің параметрлерін конфигурациялау мүмкіндігін қарастырыңыз.

Конфигурация файлының әдепкі жолы: `C:\Program Files\PostgreSQL\<НҰСҚА>\data\postgresql.conf`

PostgreSQL және Postgres Pro үшін ұсынылатын параметрлер:

- `max_connections = 151`
- `shared_buffers = N`

  ДҚБЖ орнатылған құрылғының жедел жады көлемінің N = 25 пайызы Егер жедел жад 1 ГБ-тан аз болса, онда әдепкі бойынша мәнді қалдырыңыз.
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `maintenance_work_mem = 128MB`
- `max_stack_depth = 2MB`
- `max_parallel_workers_per_gather = 0`
- `standard_conforming_strings = on`

Postgres Pro 15.7 немесе Postgres Pro 15.7.1 пайдалансаңыз, `enable_compound_index_stats` опциясын өшіріңіз:

```
enable_compound_index_stats = off
```

Конфигурацияны қолданыңыз немесе конфигурация файлын жаңартқаннан кейін ДҚБЖ серверін қайта іске қосыңыз.

PostgreSQL және Postgres Pro серверінің параметрлері, сондай-ақ осы параметрлерді қалай көрсету керектігі туралы толық ақпаратты ДҚБЖ бойынша тиісті құжаттамадан қараңыз.

PostgreSQL және Postgres Pro үшін есептік жазбаларды жасау және конфигурациялау туралы қосымша ақпаратты келесі бөлімінен қараңыз: PostgreSQL және Postgres Pro бағдарламаларымен жұмыс істеу үшін есептік жазбаларды конфигурациялау.

Сенімділігі жоғары кластерге қолдау көрсету

Қолжетімділігі жоғары PostgreSQL кластерлеріне келесі параметрлермен қолдау көрсетіледі:

- Репликация түрі: синхронды
- Түйіндердің минималды саны: 3
- Түйіндердің максималды саны: 15

Функцияны пайдалану үшін келесі пәрменді орындау арқылы KLCS_FF_SUPPORT_POSTGRES_FAIILOVER жалаушасын қосыңыз:

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv ".core/.independent" -s klcsff -n
KLCS_FF_SUPPORT_POSTGRES_FAIILOVER -t d -v 1
```

ДҚБЖ-ға қол жеткізу үшін сервер пайдаланатын Postgres рөлі келесі көріністерді оқу құқықтарына ие болуы керек (әдепкі бойынша қосулы):

- pg_stat_replication
- pg_stat_wal_receiver

Kaspersky Endpoint Security for Android орнатылған ұялы құрылғыларын басқару

Kaspersky Endpoint Security for Android орнатылған (бұдан әрі KES құрылғылары) ұялы құрылғыларды басқару Басқару сервері арқылы жүргізіледі. Kaspersky Security Center KES құрылғыларды басқарудың келесі мүмкіндіктеріне қолдау көрсетеді:

- Ұялы құрылғылармен клиент құрылғысына ұқсас жұмыс істеу:
  - Басқару топтарына мүшелік
  - Мониторинг, мысалы күйлерді, оқиғаларды және есептерді қарау
  - Жергілікті параметрлерді өзгерту және Android үшін Kaspersky Endpoint Security қолданбасына арналған саясаттарды тағайындау
- Пәрмендерді орталықтандырылған жіберу
- Ұялы қолданбалар пакетін қашықтан орнату

Басқару сервері KES құрылғыларды TLS протоколы, 13292 TCP-порты арқылы басқарады.

Басқару серверіне интернеттен қатынасуды ұсыну

Кейбір жағдайларда интернеттен Басқару серверіне қатынасу мүмкіндігін ұсыну қажет:

- Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын үнемі жаңарту.
- Үшінші тарап бағдарламаларын жаңарту

Әдепкі бойынша, Басқару сервері Microsoft бағдарламасының жаңартуларын басқарылатын құрылғыларға орнату үшін интернет байланысын қажет етпейді. Мысалы, басқарылатын құрылғылар Microsoft бағдарламасының жаңартуларын тікелей Microsoft жаңарту серверлерінен немесе ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server серверінен жүктей алады. Басқару сервері келесі жағдайларда интернетке қосылуы керек:

- Басқару серверін WSUS сервері ретінде пайдаланған кезде.
- Microsoft бағдарламаларынан басқа үшінші тарап бағдарламаларының жаңартуларын орнату үшін.

- Үшінші тарап бағдарламаларында осалдықтарды түзету

  Басқару серверін интернетке қосу келесі тапсырмаларды орындау үшін қажет:

  - Microsoft бағдарламалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді Kaspersky мамандары қалыптастырады және үнемі жаңартып отырады.
  - Microsoft қолданбаларынан басқа үшінші тарап қолданбаларындағы осалдықтарды түзету.

- Автономды пайдаланушылардың құрылғыларын (ноутбуктарын) басқару үшін.
- Қашықтағы кеңселердегі құрылғыларды басқару үшін.
- Қашықтағы кеңселерде орналасқан негізгі немесе қосалқы Басқару серверлерімен өзара әрекеттесу кезінде.
- ұялы құрылғыларды басқару үшін

Бұл бөлімде интернеттен Басқару серверіне қатынасуды қамтамасыз етудің типтік тәсілдері қарастырылған. Интернеттен Басқару серверіне қатынасуды қамтамасыз етудің барлық жағдайларында Басқару серверіне арнайы сертификат белгілеу қажет болуы мүмкін.

Интернеттен қатынасу: жергілікті желідегі Басқару сервері

Басқару сервері ұйымның ішкі желісінде орналасса, сіз 13000 TCP Басқару серверінің портын "Port Forwarding" механизмі арқылы сырттан қолжетімді ете аласыз. Ұялы құрылғыларды басқару қажет болса, сіз 13292 TCP портын қолжетімді ете аласыз.

Интернеттен қатынасу: Демилитаризацияланған аймақтағы Басқару сервері

Басқару сервері ұйым желісінің демилитаризацияланған аймағында орналасса, онда ол ұйымның ішкі желісіне қатынаса алмайды. Соның салдарынан, келесі шектеулер қойылады:

- Басқару сервері жаңа құрылғыларды өз бетінше анықтай алмайды.
- Басқару сервері ұйымның ішкі желісінің құрылғыларына мәжбүрлеп орнату арқылы Желілік агентті бастапқы орналастыруды орындай алмайды.

Мәселе тек Желілік агентті бастапқы орнату туралы. Желілік агент нұсқасының кейінгі жаңартуларын немесе қауіпсіздік бағдарламасын орнатуды Басқару сервері жүзеге асыра алады. Алайда, Желілік агенттерді бастапқы орналастыру басқа құралдармен жүзеге асырылуы мүмкін, мысалы, Microsoft Active Directory топтық саясатының көмегімен.

- Басқару сервері басқарылатын құрылғыларға 15000 UDP портына хабарландыру жібере алмайды, бұл Kaspersky Security Center үшін маңызды емес.
- Басқару сервері Active Directory сауалнамасын жүргізе алмайды. Дегенмен, Active Directory сауалнамасының нәтижелері көптеген сценарийлерде қажет емес.

Егер жоғарыда сипатталған шектеулер өте маңызды болса, олар ұйымның желісінде орналасқан тарату нүктелерінің көмегімен алынып тасталуы мүмкін:

- Бастапқы орналастыруды Желілік агенті жоқ құрылғыларда орындау үшін алдымен Желілік агентті құрылғылардың біріне орнатып, сол құрылғыны тарату нүктесіне тағайындау керек. Нәтижесінде, Желілік агентті басқа құрылғыларға бастапқы орнатуды осы тарату нүктесі арқылы Басқару сервері жүзеге асырады.

- Ұйымның ішкі желісінде жаңа құрылғыларды табу және Active Directory сауалнамасын жүргізу үшін тарату нүктелерінің бірінде желінің қажетті сауалнамасы түрлерін қосу керек.

Хабарландыруларды ұйымның ішкі желісінде орналасқан басқарылатын құрылғыларға 15000 UDP портына сәтті жіберу үшін кәсіпорынның бүкіл желісін тарату нүктелерімен қамту керек. Тағайындалған тарату нүктелерінің сипаттарында **Басқару серверімен байланысты үзбеу** жалаушасын қойыңыз. Нәтижесінде, Басқару сервері тарату нүктелерімен тұрақты байланысады, ал тарату нүктелері хабарландыруларды ұйымның ішкі желісінде орналастырылған құрылғыларға 15000 UDP портына жібере алады (бұл IPv4 желісі немесе IPv6 желісі болуы мүмкін).

Интернеттен қатынасу: Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану

Басқару сервері ұйымның ішкі желісінде орналасуы мүмкін, ал желінің демилитаризацияланған аймағында кері қосылым бағыты бар қосылым шлюзі ретінде жұмыс істейтін Желілік агенті бар құрылғы орналасуы мүмкін (Басқару сервері Желілік агентпен қосылым орнатады). Бұл жағдайда, интернеттен қатынасуды ұйымдастыру үшін келесі шарттарды орындау қажет:

- Желілік агент демилитаризацияланған аймақтағы құрылғыға орнатылуы керек. Желілік агентті орнату кезінде орнату шеберінің **Қосылым шлюзі** терезесінде **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** тармағын таңдаңыз.

- Қосылым шлюзі орнатылған құрылғысын тарату нүктесі ретінде қосуға болады. Қосылым шлюзін қоссаңыз, **Тарату нүктесін қосу** терезесінде **Таңдау** → **Келесі мекенжай бойынша демилитаризацияланған аймақта орналасқан қосылымдар шлюзін қосу** параметрін таңдаңыз.

- Сыртқы компьютер құрылғыларын басқару серверіне қосу мақсатымен интернетті пайдалану үшін желілік агенттің орнату пакетін түзету керек. Жасалған орнату пакетінің сипаттарында **Қосымша** →**Басқару серверіне байланыс шлюзі арқылы қосылу** параметрін таңдап, жаңадан жасалған қосылым шлюзін көрсетіңіз.

Демилитаризацияланған аймақта орналасқан қосылым шлюзі үшін Басқару сервері Басқару серверінің сертификаты қол қойған сертификатты жасайды. Егер әкімші Басқару серверіне пайдаланушы сертификатын белгілеу туралы шешім қабылдаса, онда мұны демилитаризацияланған аймақта қосылым шлюзін жасамас бұрын жасау керек.

Егер жергілікті желіден де, интернеттен де Басқару серверіне қосыла алатын ноутбуктері бар қызметкерлер болса, Желілік агент саясатында Желілік агентті ауыстыру ережесін құрған жөн.

Тарату нүктелері туралы

Желілік агенті орнатылған құрылғыларды тарату нүктесі ретінде пайдалануға болады. Бұл режимде, Желілік агент келесі функцияларды орындай алады:

- Жаңартуларды тарату, бұл арада жаңартуларды Басқару серверінен де, Kaspersky серверлерінен де алуға болады. Соңғы жағдайда, тарату нүктесі болып табылатын құрылғы үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы жасалуы тиіс:
    - Бағдарламалық жасақтаманы басқа құрылғыларға орнату, соның ішінде құрылғыларда Желілік агенттерді бастапқы орналастыруды орындау.
    - Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

Тарату нүктелерін ұйымның желісіне орналастыру келесі мақсаттарды көздейді:

- Басқару серверіне түсетін жүктемені азайту.
- Трафикті оңтайландыру.
- Басқару серверіне ұйым желісінің жетуі қиын бөліктеріндегі құрылғыларға қатынасу мүмкіндік беру. NAT артында орналасқан тарату нүктесінің болуы (Басқару серверіне қатысты) Басқару серверіне келесі әрекеттерді орындауға мүмкіндік береді:
    - IPv4 немесе IPv6 желілеріндегі UDP арқылы құрылғыларға хабарландырулар жіберу
    - IPv4 немесе IPv6 желісінде сауалнама өткізу
    - Бастапқы орналастыруды орындау
    - push-сервер ретінде қолдану

Тарату нүктесі басқару тобына тағайындалады. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымы осы басқару тобындағы және оның барлық ішкі топтарындағы құрылғылар болады. Бұл ретте, тарату нүктесі болып табылатын құрылғы ол тағайындалған басқару тобында болуға міндетті емес.

Сіз тарату нүктесін қосылым шлюзі етіп жасай аласыз. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымындағы құрылғылар Басқару серверіне тікелей емес, шлюз арқылы қосылады. Бұл режим, Басқару сервері мен басқарылатын құрылғылар арасында тікелей қосылым мүмкін болмайтын сценарийлерде пайдалы.

Linux басқаруымен жұмыс істейтін құрылғыны тарату нүктесі ретінде пайдалансаңыз, klnagent қызметі үшін файл дескрипторының шектеулерін ұлғайту ұсынылады, себебі тарату нүктесінің әрекет ету ауқымы көптеген құрылғыларды қамтыса, әдепкі бойынша ашылуы мүмкін файлдардың ең көп саны жетпей қалуы ықтимал.

klnagent қызметі үшін файл дескрипторларының шектеуін арттыру

Егер Linux басқаруымен жұмыс істейтін тарату нүктесінің тарату аймағы көптеген құрылғыларды қамтыса, ашық файлдар санына (файл дескрипторлары) әдепкі түрде қойылатын шектеу жеткіліксіз болуы мүмкін. Бұған жол бермеу үшін klnagent қызметі үшін файл дескрипторының шектеуін арттыруға болады.

klnagent қызметі үшін файл дескрипторының шектеуін арттыру үшін

1. Тарату нүктесі ретінде әрекет ететін Linux негізіндегі құрылғыда келесі пәрменді орындаңыз:

   ```
   systemctl edit klnagent64.service
   ```

2. `[Service]` бөлімінің `LimitNOFILE` параметрінде файл дескрипторларының қатаң және жұмсақ шектерін көрсетіңіз:

   `LimitNOFILE=<жұмсақ ресурс шегі>:<қатты ресурс шегі>`

   Мысалы, `LimitNOFILE=32768:131072`. Файл дескрипторының жұмсақ шектеулері қатаң шектеуден аз немесе оған тең болуы керек екенін ескеріңіз.

3. Параметрлердің дұрыстығына көз жеткізу үшін келесі пәрменді іске қосыңыз:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Параметрлер қате көрсетілген болса, бұл пәрмен келесі қателердің бірін тудыруы мүмкін:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Егер бұл қате орын алса, демек, `LimitNOFILE` жолындағы таңбалар дұрыс көрсетілмеген. Енгізілген жолды тексеру және түзету қажет.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Бұл қате орын алса, сіз енгізген файл дескрипторларын жұмсақ шектеу қатаң шектеуден асып кетеді. Енгізілген жолды тексеріп, файл дескрипторының жұмсақ шектеуі қатаң шектеуден аз немесе оған тең екеніне көз жеткізу керек.

4. systemd процесін қайта бастау үшін келесі пәрменді іске қосыңыз:

   ```
   systemctl daemon-reload
   ```

5. Желілік агент қызметін қайта іске қосу үшін келесі пәрменді орындаңыз:

   ```
   systemctl restart klnagent
   ```

6. Көрсетілген параметрлердің дұрыс қолданылғанына көз жеткізу үшін келесі пәрменді орындаңыз:

   `less /proc/<nagent процесінің идентификаторы>/limits`

   мұндағы `<nagent процесінің идентификаторы>` параметрі — желілік агент процесінің идентификаторы. Сәйкестендіргішті алу үшін келесі пәрменді орындауыңызға болады:

   ```
   ps -ax | grep klnagent
   ```

Linux операциялық жүйесімен жұмыс істейтін тарату нүктесі үшін ашылатын файлдар саны ұлғайтылды.

Тарату нүктелерінің саны мен конфигурациясын есептеу

Желіде клиент құрылғылары неғұрлым көп болса, тарату нүктелері да соғұрлым көп қажет болады. Тарату нүктелерін автоматты түрде тағайындауды өшірмеу ұсынылады. Тарату нүктелерін автоматты түрде тағайындау қосылған кезде, егер клиент құрылғыларының саны айтарлықтай көп болса, Басқару сервері тарату нүктелерін тағайындайды және олардың конфигурациясын анықтайды.

Арнайы бөлінген тарату нүктелерін пайдалану

Егер сіз тарату нүктелері ретінде белгілі бір құрылғыларды (мысалы, бұл үшін бөлінген серверлер) пайдалануды жоспарласаңыз, онда тарату нүктелерін автоматты түрде тағайындауды пайдаланбауға болады. Бұл жағдайда, тарату нүктелері ретінде тағайындағыңыз келетін құрылғыларда дискіде жеткілікті бос орын бар екеніне, олар үнемі өшірілмейтініне және "ұйқы режимі" өшірілгеніне көз жеткізіңіз.

Желілік құрылғылардың санына байланысты бір сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Желілік құрылғылардың санына байланысты бірнеше сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–100	1
100-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Клиент құрылғыларын (жұмыс станцияларын) тарату нүктелері ретінде пайдалану

Егер сіз әдеттегі клиент құрылғысын (жұмыс станциясын) тарату нүктесі ретінде пайдалануды жоспарласаңыз, байланыс арналары мен Басқару серверіне шамадан тыс жүктемені болдырмау үшін төмендегі кестеде көрсетілгендей тарату нүктесін тағайындау ұсынылады:

Желілік құрылғылардың санына байланысты желінің бір сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Желілік құрылғылардың санына байланысты желінің бірнеше сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–30	1
31–300	2
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Егер тарату нүктесі өшірілген болса немесе басқа себептерге байланысты қолжетімді болмаса, онда басқарылатын құрылғылар жаңартулар алу үшін осы тарату нүктесінің әрекет ету ауқымынан Басқару серверіне жүгіне алады.

Басқару серверлерінің иерархиясы

MSP-де бірден артық Басқару сервері болуы мүмкін. Бірнеше шашыраңқы Серверлерді басқару ыңғайсыз, сондықтан оларды иерархияға біріктірген жөн. Екі Басқару сервері арасындағы "негізгі – қосалқы" өзара іс-қимылы келесі мүмкіндіктер ұсынады:

- Қосалқы Сервер басты Серверден саясаттар мен тапсырмаларды иеленеді, параметрлердің қайталануы жойылады.
- Басқару сервердегі құрылғыны таңдауларға қосалқы Басқару серверлердегі құрылғылар қосылуы мүмкін.
- Басты Басқару сервердегі есептерге қосалқы Басқару серверлердегі деректер (соның ішінде егжей-тегжейлі) қосылуы мүмкін.

Негізгі Басқару сервері жоғарыда берілген параметрлер аясында деректерді виртуалды емес, тәуелді басқару серверлерінен ғана алады. Бұл шектеулер негізгі басқару серверімен бір дерекқорды пайдаланатын виртуалды басқару серверлеріне қолданылмайды.

Виртуалды Басқару серверлері

Физикалық Басқару серверінің шеңберінде бірнеше виртуалды Басқару серверлерін құруға болады, олардың көпшілігі қосалқы Серверлерге ұқсас. Қатынасуды бақылау тізіміне (ACL) негізделген қатынасуды бөлу моделімен салыстырғанда, виртуалды Серверлер моделі анағұрлым функционалды болып келеді және оқшаулаудың үлкен дәрежесін ұсынады. Саясат пен тапсырма құрылғыларына тағайындауға арналған басқару топтарының құрылымынан басқа, әрбір виртуалды Басқару серверінің өзіндік тағайындалмаған құрылғылар тобы, өзіндік есептер жиынтығы, құрылғыларды таңдау және оқиғалар, орнату пакеттері, жылжыту ережелері және т.б. бар. Виртуалды Басқару серверлерінің функционалдығы, әртүрлі клиенттерді бір-бірінен барынша оқшаулау үшін провайдерлер (xSP) тарапынан, сондай-ақ күрделі құрылымы және көптеген әкімшілері бар ірі ұйымдар тарапынан қолданылуы мүмкін.

Виртуалды Серверлер көбінесе қосалқы Басқару серверлеріне ұқсас болып келеді, алайда олардың келесі айырмашылықтары бар:

- виртуалды Серверде көптеген жаһандық параметрлер мен өзіндік TCP порттары жоқ;
- виртуалды Серверде қосалқы Серверлер болуы мүмкін емес;
- виртуалды Серверде өзінің виртуалды Серверлері болуы мүмкін емес;
- физикалық Басқару серверінде, оның барлық виртуалды Серверлерінің басқарылатын құрылғыларынан (карантин элементтері, бағдарламалар тізімдемесі және т.б.) құрылғылар, топтар, оқиғалар мен нысандар көрінеді;
- виртуалды Сервер желіні тек оған қосылған тарату нүктелері арқылы сканерлей алады.

Kaspersky Security Center шектеулері туралы ақпарат

Төмендегі кестеде Kaspersky Security Center ағымдағы нұсқасының шектеулері келтірілген.

Шектеу түрі	Мән
Бір Басқару серверіне шаққандағы басқарылатын құрылғылардың ең көп саны	100 000
Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың ең көп саны	300
Басқару топтарының ең көп саны	10 000
Сақталатын оқиғалардың ең көп саны	45 000 000
Саясаттардың ең көп саны	2000
Тапсырмалардың ең көп саны	2000
Active Directory нысандарының ең көп жиынтық саны (бөлімшелер мен пайдаланушылардың есептік жазбалары, құрылғылар және қауіпсіздік топтары)	1 000 000
Саясаттағы профильдердің ең көп саны	100
Бір негізгі Басқару серверіндегі қосалқы Серверлердің ең көп саны	500
Виртуалды Басқару серверлерінің ең көп саны	500
Бір тарату нүктесі қызмет көрсете алатын құрылғылардың ең көп саны (тарату нүктелері тек ұялы емес құрылғыларға қызмет көрсете алады)	10 000
Бір қосылымы шлюзін қолдана алатын құрылғылардың ең көп саны	10 000, ұялы құрылғылармен қоса
Бір Басқару серверіне шаққандағы ұялы құрылғылардың ең көп саны	100 000 минус тұрақты басқарылатын құрылғылар саны

Желіге түсетін жүктеме

Бұл бөлімде, өзекті басқару сценарийлерін орындау барысында клиент құрылғылары мен Басқару сервері өзара алмасатын желілік трафиктің көлемі туралы ақпарат келтіріледі.

Желіге түсетін негізгі жүктеме келесі басқару сценарийлерін орындаумен байланысты:

- Антивирустық қорғанысты алғашқы рет орналастыру
- Антивирустық дерекқорларды алғашқы рет жаңарту
- Клиент құрылғысын Басқару серверімен синхрондау
- Антивирустық дерекқорларды үнемі жаңартып тұру
- Клиент құрылғыларындағы оқиғаларды Басқару серверінің өңдеуі

Антивирустық қорғанысты алғашқы рет орналастыру

Бұл бөлімде, клиент құрылғысына Желілік агент нұсқасы мен Kaspersky Endpoint Security for Windows бағдарламасын орнату кезіндегі трафик шығыны келтірілген (төмендегі кестені қараңыз).

Желілік агент, Басқару сервері орнатуға қажетті файлдарды клиент құрылғысындағы ортақ қатынасы бар қалтаға көшіру кезінде күшпен орнату арқылы орнатылады. Орнатып болғаннан кейін, Желілік агент Басқару серверімен орнатылған қосылымды қолдана отырып, Kaspersky Endpoint Security for Windows дистрибутивін алады.

Сценарий	Желілік агентті бір клиент құрылғысы үшін орнату	Kaspersky Endpoint Security for Windows бағдарламасын бір клиент құрылғысы үшін орнату (жаңартылған дерекқорлармен)	Желілік агент пен Kaspersky Endpoint Security for Windows бағдарламасын бірлесіп орнату
Клиент құрылғысынан Басқару серверіне дейінгі трафик, КБ	1638,4	7843,84	9707,52
Басқару серверінен клиент құрылғысына дейінгі трафик, КБ	69 990,4	259 317,76	329 318,4
Жалпы трафик (бір клиент құрылғысы үшін), КБ	71 628,8	267 161,6	339 025,92

Желілік агенттерді клиент құрылғыларына орнату үшін басқару тобындағы құрылғылардың бірін тарату нүктесі ретінде тағайындауға болады. Ол орнату пакеттерін тарату үшін қолданылады. Бұл жағдайда, антивирустық қорғанысты алғашқы рет орналастыру кезінде жіберілетін трафик көлемі, көп мекенжайлы IP таратылымының қолданылып-қолданылмайтынына байланысты айтарлықтай ерекшеленеді.

Көп мекенжайлы IP таратылымын қолданған жағдайда, орнату пакеттері басқару тобындағы барлық қосылған құрылғыларға бір рет таратылады. Осылайша, жалпы трафик шамамен N есе азаяды, мұндағы N – басқару тобында қосылған құрылғылардың жалпы саны. Көп мекенжайлы IP таратылым қолданылмаса, жалпы трафик Басқару серверінен дистрибутивтерді жүктеп алу трафигіне сай келеді. Бұл арада, орнату пакеттерінің көзі – Басқару сервері емес, тарату нүктесі болып табылады.

Антивирустық дерекқорларды алғашқы рет жаңарту

Антивирустық дерекқорларды алғашқы рет жаңарту (клиент құрылғысында жаңарту тапсырмасын бірінші рет іске қосу) кезіндегі трафик жылдамдығы келесідей:

- Клиент құрылғысынан Басқару серверіне дейінгі трафик: 1.8 МБ.
- Басқару серверінен клиент құрылғысына дейінгі трафик: 113 МБ.
- Жалпы трафик (бір клиент құрылғысы үшін): 114 МБ.

Деректер антивирустық дерекқордың ағымдағы нұсқасына байланысты біршама ерекшеленуі мүмкін.

Клиентті Басқару серверімен синхрондау

Бұл сценарий, клиент құрылғысы мен Басқару сервері арасындағы деректер белсенді түрде синхрондалып жатқан кездегі басқару жүйесінің күйін сипаттайды. Клиент құрылғылары Басқару серверіне әкімші белгілеген кезеңмен қосылады. Басқару сервері клиент құрылғысындағы деректердің күйін Сервердегі деректердің күйімен салыстырады, дерекқорда клиент құрылғысын соңғы рет қосу туралы деректерді тіркейді және деректерді синхрондайды.

Бұл бөлімде клиентті басқару серверіне қосу кезінде негізгі басқару сценарийлеріне арналған трафик мәндері туралы ақпарат берілген (төмендегі кестені қараңыз). Кестедегі деректер антивирустық дерекқордың ағымдағы нұсқасына байланысты біршама ерекшеленуі мүмкін.

Трафик шығыны

Сценарий	Клиент құрылығыларынан Басқару серверіне дейінгі трафик, КБ	Басқару серверінен клиент құрылғыларына дейінгі трафик, КБ	Жалпы трафик (бір клиент құрылғысы үшін), КБ
Клиент құрылғысында дерекқорларды жаңартуға дейін алғашқы рет синхрондау	699,44	568,42	1267,86
Клиент құрылғысында дерекқорларды жаңартқаннан кейін алғашқы рет синхрондау	735,8	4474,88	5210,68

Клиент құрылғысы мен Басқару серверінде өзгерістер болмаған кезде синхрондау	11,99	6,73	18,72
Топ саясатында бір параметр өзгерген кезде синхрондау	9,79	11,39	21,18
Топтық тапсырмада бір параметр өзгерген кезде синхрондау	11,27	11,72	22,99
Клиент құрылғысында өзгерістер болмаған кезде күштеп синхрондау	77,59	99,45	177,04

Жалпы трафиктің көлемі, басқару топтарының ішінде көп мекенжайлы IP таратылымының қолданылып-қолданылмауына байланысты айтарлықтай өзгереді. Мекенжайлы IP таратылымын қолданған жағдайда, топ үшін жалпы трафик шамамен N есе азаяды, мұндағы N – басқару тобындағы қосылған құрылғылардың саны.

Бастапқы синхрондау кезінде дерекқорларды жаңартуға дейінгі және одан кейінгі трафик көлемі келесі жағдайлар үшін көрсетілген:

- Желілік агент пен қауіпсіздік бағдарламаларын клиент құрылғысына орнату;
- клиент құрылғысын басқару тобына көшіру;
- клиент құрылғысына әдепкі бойынша топ үшін жасалған саясат пен тапсырмаларды қолдану.

Кестеде Kaspersky Endpoint Security саясатының параметрлеріне кіретін қорғаныс параметрлерінің бірі өзгерген кездегі трафик көлемі көрсетілген. Саясаттың басқа параметрлеріне арналған деректер кестеде көрсетілген деректерден ерекшеленуі мүмкін.

Антивирустық дерекқорларды қосымша жаңарту

Алдыңғы жаңартудан 20 сағат өткен соң антивирустық дерекқорларды инкрементті түрде жаңарту кезіндегі трафик шығыны келесідей:

- Клиент құрылғысынан Басқару серверіне дейінгі трафик: 169 КБ.
- Басқару серверінен клиент құрылғысына дейінгі трафик: 16 МБ.
- Жалпы трафик (бір клиент құрылғысы үшін): 16.3 МБ.

Кестедегі деректер антивирустық дерекқордың ағымдағы нұсқасына байланысты біршама ерекшеленуі мүмкін.

Трафиктің көлемі, басқару топтарының ішінде көп мекенжайлы IP таратылымының қолданылып-қолданылмауына байланысты айтарлықтай өзгереді. Мекенжайлы IP таратылымын қолданған жағдайда, топ үшін жалпы трафик шамамен N есе азаяды, мұндағы N – басқару тобындағы қосылған құрылғылардың саны.

Клиенттердің оқиғаларын Басқару серверінің өңдеуі

Бұл бөлімде, клиент құрылғысында "Вирус табылды" оқиғасы орын алған кездегі трафиктің шығыны келтірілген, ол туралы ақпарат Басқару серверіне жіберіледі және дерекқорде тіркеледі (төмендегі кестені қараңыз).

Сценарий	"Вирус табылды" оқиғасы басталған кезде деректерді Басқару серверіне беру	Тоғыз "Вирус табылды" оқиғасы басталған кезде деректерді Басқару серверіне беру
Клиент құрылғысынан Басқару серверіне дейінгі трафик, КБ	49,66	64,05
Басқару серверінен клиент құрылғысына дейінгі трафик, КБ	28,64	31,97
Жалпы трафик (бір клиент құрылғысы үшін), КБ	78,3	96,02

Кестедегі деректер, антивирустық бағдарламаның ағымдағы нұсқасына байланысты және саясатта қандай оқиғалар Басқару серверінің дерекқорында тіркеуді қажет ететін деп анықталғанына байланысты біршама өзгеруі мүмкін.

Тәулік ішіндегі трафик шығыны

Бұл бөлімде клиент құрылғылары немесе басқару сервері деректерге өзгерістер енгізбеген "тыныш" күйдегі басқару жүйесінің 24 сағаттық әрекетіндегі трафик жылдамдығы туралы ақпарат берілген (төмендегі кестені қараңыз).

Кестедегі деректер Kaspersky Security Center бағдарламасын стандартты түрде орнатқаннан және бағдарламаны жылдам іске қосу шеберін жапқаннан кейінгі желінің күйін сипаттайды. Клиент құрылғысының Басқару серверімен синхрондалу кезеңі 20 минутты құрады, жаңартуларды Басқару серверінің қоймасына жүктеп алу сағат сайын жүзеге асырылып тұрды.

Тыныш күйдегі бір тәуліктегі трафик деңгейі

Трафик ағыны	Мән
Клиент құрылғысынан Басқару серверіне дейінгі трафик, КБ	3235,84
Басқару серверінен клиент құрылғысына дейінгі трафик, КБ	64 378,88
Жалпы трафик (бір клиент құрылғысы үшін), КБ	67 614,72

Ұялы құрылғыларды басқаруға дайындық

Бұл бөлімде келесі ақпарат бар:

- мамандандырылған iOS MDM профильдерін орнату арқылы iOS құрылғыларын басқаруға арналған iOS MDM сервері туралы;
- Kaspersky Endpoint Security for Android қолданбасы орнатылған ұялы құрылғыларды басқару туралы.

iOS MDM сервері

iOS MDM сервері оларға мамандандырылған iOS MDM-профильдерін орнату арқылы iOS-құрылғыларды басқаруға мүмкіндік береді. Келесі функцияларға қолдау көрсетіледі:

- құрылғыны бұғаттау;
- құпиясөзді бастапқы қалпына келтіру;
- құрылғының деректерін жою;

- қолданбаларды орнату немесе жою;
- қосымша параметрлері бар iOS MDM-профильді пайдалану (мысалы, VPN, пошта, Wi-Fi, камера параметрлері, сертификаттар және тағы басқасы).

iOS MDM сервері TLS-портына (әдепкі бойынша 443 порты) ұялы құрылғылардан кіріс қосылымдарды қабылдайтын және Желілік агент арқылы Kaspersky Security Center тарапынан басқарылатын веб-қызмет болып табылады. Желілік агент жергілікті түрде iOS MDM сервері орналастырылған құрылғыға орнатылады.

iOS MDM серверін орналастыру процесінде әкімшіге келесі әрекеттерді орындау қажет:

- Желілік агенттің Басқару серверіне қатынасын қамтамасыз ету;
- ұялы құрылғылардың iOS MDM серверінің TCP-портына қатынасын қамтамасыз ету.

Бұл бөлімде iOS MDM серверінің екі типтік конфигурациялары қарастырылған.

Типтік конфигурация: демилитаризацияланған аймақтағы Kaspersky Device Management for iOS

iOS MDM сервері интернетке қатынасу мүмкіндігі бар ұйым желісінің демилитаризацияланған аймағында орналасқан. Бұл тәсілдің ерекшелігі, құрылғылар тарапынан интернеттен iOS MDM веб-қызметінің қолжетімділігіне қатысты мәселелердің болмауы.

iOS MDM серверін басқару үшін жергілікті орнатылған Желілік агент қажет болғандықтан, бұл Желілік агенттің Басқару серверімен өзара әрекеттесуін қамтамасыз ету қажет. Мұны келесі тәсілдермен жасауға болады:

- Басқару серверін демилитаризацияланған аймаққа орналастырыңыз.
- Қосылымдар шлюзін қолдану:
  a. Орналастырылған iOS MDM сервері бар құрылғыда Желілік агентті қосылым шлюзі арқылы Басқару серверіне қосу.
  b. iOS MDM сервері орналастырылған құрылғыда Желілік агентті қосылым шлюзі етіп тағайындау.

Типтік конфигурация: ұйымның жергілікті желісіндегі iOS MDM сервері

iOS MDM сервері ұйымның ішкі желісінде орналасады. 443 порты (әдепкі порт) сырттан қол жетімді болуы керек, мысалы, iOS MDM веб-қызметін Kerberos Constrained Delegation пайдалануды қолдайтын кері прокси-серверде жариялау арқылы.

Кез келген типтік конфигурацияда TCP 2197 порты бойынша Apple веб-сервистерінің (17.0.0.0/8 мекенжайлар ауқымы) iOS MDM Сервері үшін қолжетімділікті қамтамасыз ету керек. Бұл порт APNs мамандандырылған сервисі арқылы жаңа пәрмендер туралы құрылғыларға хабарлау үшін пайдаланылады.

Kaspersky Endpoint Security for Android орнатылған ұялы құрылғыларын басқару

Kaspersky Endpoint Security for Android орнатылған (бұдан әрі KES құрылғылары) ұялы құрылғыларды басқару Басқару сервері арқылы жүргізіледі. Kaspersky Security Center KES құрылғыларды басқарудың келесі мүмкіндіктеріне қолдау көрсетеді:

- Ұялы құрылғылармен клиент құрылғысына ұқсас жұмыс істеу:
  - Басқару топтарына мүшелік
  - Мониторинг, мысалы күйлерді, оқиғаларды және есептерді қарау
  - Жергілікті параметрлерді өзгерту және Android үшін Kaspersky Endpoint Security қолданбасына арналған саясаттарды тағайындау
- Пәрмендерді орталықтандырылған жіберу
- Ұялы қолданбалар пакетін қашықтан орнату

Басқару сервері KES құрылғыларды TLS протоколы, 13292 TCP-порты арқылы басқарады.

Басқару серверінің өнімділігі туралы мәліметтер

Бөлімде әртүрлі аппараттық конфигурациялар үшін Басқару серверінің өнімділігін тестілеу нәтижелері, сондай-ақ басқарылатын құрылғыларды Басқару серверіне қосу шектеулері келтірілген.

Басқару серверіне қосылу шектеулері

Басқару сервері өнімділікті жоғалтпай, 100 000 құрылғыға дейін басқаруды қолдайды.

Өнімділікті жоғалтпай Басқару серверіне қосылуға шектеулер:

- Бір Басқару сервері 500-ге дейін виртуалды Басқару серверін қолдай алады.
- Негізгі Басқару сервері бір уақытта ең көбі 1000 сеансқа қолдау көрсетпейді.
- Виртуалды Басқару сервері бір уақытта ең көбі 1000 сеансқа қолдау көрсетеді.

Басқару серверінің өнімділігін тестілеу нәтижелері

Басқару серверінің өнімділік тестілерінің нәтижелері, Басқару сервері көрсетілген уақыт аралығы ішінде синхрондауды орындай алған клиент құрылғыларының ең көп санын анықтауға мүмкіндік берді. Сіз осы ақпаратты антивирустық қорғанысты компьютерлік желілерде орналастырудың оңтайлы схемасын таңдау үшін қолдана аласыз.

Тестілеу үшін келесі аппараттық конфигурациялары бар құрылғылар қолданылады (төмендегі кестелерді қараңыз):

Басқару серверінің аппараттық конфигурациясы

Параметр	Мән
Процессор	Intel Xeon CPU E5630, тактілік жиілігі 2,53 ГГц, 2 сокет, 8 ядро, 16 логикалық процессор
ЖЖҚ	26 ГБ
Қатты диск	IBM ServeRAID M5014 SCSI Disk Device, 487 ГБ
Операциялық жүйе	Microsoft Windows Server 2019 Standard, нұсқасы 10.0.17763, жинағы 17763
Желі	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

SQL Server бар құрылғының аппараттық конфигурациясы

Параметр	Мән
Процессор	Intel Xeon CPU X5570, тактілік жиілігі 2,93 ГГц, 2 сокет, 8 ядро, 16 логикалық процессор
ЖЖҚ	32 ГБ
Қатты диск	Adaptec Array SCSI Disk Device, 2047 ГБ
Операциялық жүйе	Microsoft Windows Server 2019 Standard, нұсқасы 10.0.17763, жинағы 17763
Желі	Intel 82576 Gigabit

Басқару сервері 500 виртуалды Басқару серверін жасауды қолдады.

Синхрондау кезеңі әрбір 10 000 басқарылатын құрылғыға 15 минуттан құрады (төмендегі кестені қараңыз).

Басқару серверін жүктеп тестілеудің жалпылама нәтижелері

Синхрондау кезеңі, мин	Басқарылатын құрылғылардың саны
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

Басқару серверін MySQL және SQL Express дерекқор серверіне қосқан кезде 10 000-нан астам құрылғыны басқаруға арналған бағдарламаны пайдалану ұсынылмайды. MariaDB дерекқорларын басқару жүйесі үшін басқарылатын құрылғылардың ең көп ұсынылатын саны 20 000 құрайды.

KSN прокси-серверінің өнімділігін тексеру нәтижелері

Егер сіздің корпоративтік желіңізде көптеген клиент құрылғылары болса және олар Басқару серверін KSN прокси-сервері ретінде пайдаланса, Басқару сервері клиент құрылғыларынан келген сұрауларды өңдеу үшін белгілі бір аппараттық талаптарды қанағаттандыруы керек. KSN прокси-сервері қызметінің қалыпты жұмысын қамтамасыз ету үшін желідегі Басқару серверінің жүктелуін бағалау және аппараттық ресурстарды жоспарлау үшін төмендегі тестілеу нәтижелерін пайдалануға болады.

Төмендегі кестеде Басқару сервері мен SQL Server серверінің аппараттық конфигурациясы берілген. Бұл конфигурация тестілеу үшін пайдаланылды.

Басқару серверінің аппараттық конфигурациясы

Параметр	Мән
Процессор	Intel Xeon CPU E5450, тактілік жиілігі 3,00 ГГц, 2 сокет, 8 ядро, 16 логикалық процессор
ЖЖҚ	32 ГБ
Операциялық жүйе	Microsoft Windows Server 2016 Standard

SQL Server аппараттық конфигурациясы

Параметр	Мән
Процессор	Intel Xeon CPU E5450, тактілік жиілігі 3,00 ГГц, 2 сокет, 8 ядро, 16 логикалық процессор
ЖЖҚ	32 ГБ
Операциялық жүйе	Microsoft Windows Server 2019 Standard

Төмендегі кестеде тестілеу нәтижелері келтірілген.

KSN прокси-серверінің өнімділігін тексерудің жалпылама нәтижелері

Параметр	Мән
Секундына өңделген сұраулардың максималды саны	4914
Орталық процессорды барынша пайдалану	36%

Сыртқы қызметтермен әрекеттесуге арналған желі параметрлері

Kaspersky Security Center жүйесі сыртқы қызметтермен әрекеттесу үшін келесі желі параметрлерін пайдаланады.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com	Бағдарламаны белсендіру.
Порт: 443 Протокол: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Kaspersky дерекқорлары, бағдарламалық жасақтама модульдеріне мен бағдарламаларын арналған жаңартулар.
Порт: 443 Протокол: HTTPS	https://downloads.upd.kaspersky.com	• Kaspersky дерекқорлары, бағдарламалық жасақтама модульдеріне мен бағдарламаларын арналған жаңартулар. • Kaspersky серверлерінің қолжетімділігін тексеру. Kaspersky Security Center бағдарламасы Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктемес бұрын Kaspersky серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Kaspersky дерекқорлары, бағдарламалық жасақтама модульдеріне мен бағдарламаларын арналған жаңартулар.
Порт: 443 Протокол: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Kaspersky Security Network қолдану.
Порт: 443, 1443 Протокол: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Kaspersky Security Network қолдану.
Порт: 443 Протокол: HTTPS	click.kaspersky.com redirect.kaspersky.com	Интерфейстегі сілтемелерге өту.

Желі параметрлері	Мекенжай	Сипаттамасы
Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Бұл серверлер ашық кілттер инфрақұрылымының (PKI) бөлігі болып табылады және Kaspersky сандық қолтаңбасы сертификаттарының жарамдылық күйін тексеру үшін қажет. CRL – кері қайтарып алынған сертификаттар тізімі болып табылады. OCSP нақты уақыт режимінде нақты сертификаттың күйін сұрауға мүмкіндік береді. Бұл қызметтер сандық сертификаттармен қауіпсіз өзара әрекетті қамтамасыз етуге және ықтимал шабуылдардан қорғауға көмектеседі.
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Жарнамалық хабарландырулар.

Kaspersky Security Center сыртқы қызметтермен дұрыс өзара әрекеттесуі үшін келесі ұсыныстарды ескеріңіз:
- Ұйымыңыздың желілік жабдығында және прокси-серверінде 443 және 1443 порттарындағы шифрланбаған желілік трафикке рұқсат берілуі тиіс.
- Басқару сервері Kaspersky жаңарту серверлерімен және Kaspersky Security Network серверлерімен өзара әрекеттескен кезде сертификаттарды алмастыру арқылы желілік трафикті ұстап қалуға (MITM шабуылдары) жол бермеу қажет.

klscflag утилитасын пайдаланып, HTTP немесе HTTPS протоколы арқылы жаңартуларды жүктеп алу үшін:

1. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Жаңартуларды HTTP протоколы арқылы жүктеп алғыңыз келсе, келесі пәрмендердің бірін орындаңыз:

   - Басқару сервер орнатылған құрылғыда:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Тарату нүктесіне:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Жаңартуларды HTTPS протоколы арқылы жүктеп алғыңыз келсе, келесі пәрмендердің бірін орындаңыз:

   - Басқару сервер орнатылған құрылғыда:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Тарату нүктесіне:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Желілік агент пен қауіпсіздік бағдарламасын орналастыру

Ұйымның құрылғыларын басқару үшін құрылғыларға Желілік агентті орнату қажет. Ұйымның құрылғыларында Kaspersky Security Center таратылған қолданбасын орналастыру әдетте оларға Желілік агентті орнатудан басталады.

Microsoft Windows XP-де Желілік агент келесі операцияларды дұрыс емес орындауы мүмкін: жаңартуларды тікелей Kaspersky серверлерінен жүктеп алу (егер тарату нүктесінің рөлін орындаса); KSN прокси-сервері ретінде жұмыс істеу (егер тарату нүктесінің рөлін орындаса); және үшінші тараптардың бағдарламаларының осалдықтарын анықтау (Осалдықтар мен патчтарды басқаруды қолданған кезде).

Бастапқы орналастыру

Ұйымның құрылғыларын басқару үшін әр құрылғыға желілік агентті орнату қажет.

Windows жүйесінде жұмыс істейтін басқарылатын құрылғыға желілік агентті келесі жолдармен орнатуға болады:

- Бағдарламаларды қашықтан орнатудың үшінші тарап құралдары арқылы.
- Операциялық жүйесі және желілік агенті бар әкімшінің қатқыл дискісінің кескінін клондау арқылы, Kaspersky Security Center диск кескіндерін өңдеу үшін берген құралдарды немесе үшінші тарап құралдарын пайдалану арқылы.
- Windows топтық саясаттарына арналған стандартты Windows басқару құралдарын пайдалану арқылы; болмаса Kaspersky Security Center-дің қашықтан орнату тапсырмасындағы сәйкес арнайы опция арқылы автоматты режимде.
- Мәжбүрлі режимде, Kaspersky Security Center қашықтан орнату тапсырмасы көмегімен операциялық жүйе ресурстарын пайдалану арқылы.
- Пайдаланушыларға Kaspersky Security Center қалыптастырған автономды пакеттерге сілтемелер тарату арқылы. Автономды пакеттер, параметрлері конфигурацияланған таңдалған бағдарламалардың дистрибутивтерін қамтитын орындалатын модульдер болып табылады.
- Құрылғыларда бағдарламалардың инсталляторларын іске қосу арқылы қолмен.

Linux жүйесінде жұмыс істейтін басқарылатын құрылғыда желілік агентті келесі жолдармен бастапқы орнатуға болады:

- Басқарылатын құрылғыға SSH арқылы қосылу және қашықтан орнату тапсырмасын орындау арқылы.
- Басқарылатын құрылғыда пакет орнатуды іске қосу арқылы.

macOS операциялық жүйесі жұмыс істейтін басқарылатын құрылғыда желілік агентті келесі жолдармен бастапқы орнатуға болады:

- macOS тарату нүктесінде қашықтан орнату тапсырмасын орындау арқылы.
- Құрылғы пайдаланушыларына Kaspersky Security Center жасаған дербес пакеттерге сілтемелер жіберу арқылы. Дербес пакеттер — алдын ала анықталған параметрлері бар таңдалған қолданбалардың тарату пакеттерін қамтитын орындалатын модульдер.

Құрылғыға желілік агент орнатылғаннан кейін, осы желілік агент арқылы сол құрылғыда Kaspersky қолданбаларын қашықтан орнатуға болады. Бұл ретте, орнатылатын бағдарламаның дистрибутивін әкімші көрсеткен орнату параметрлерімен бірге жіберу, Желілік агенттер мен Басқару сервері арасындағы байланыс арналары арқылы жүзеге асырылады. Дистрибутивті жіберу үшін тарату нүктелері, көп мекенжайлы таратылым және басқа да құралдар түріндегі аралық тарату орталықтарын пайдалануға болады.

Басқарылатын желіде қолданбаларды орналастыру әдісі мен стратегиясын таңдай отырып, бірқатар факторды назарға алған жөн (тізім толық емес):

- Ұйым желісінің конфигурациясын.
- Құрылғылардың жалпы саны.
- Ұйым желісінде Active Directory доменінің мүшелері емес құрылғылардың болуы және мұндай құрылғыларда әкімші құқықтары бар бірізді есептік жазбалардың болуы.
- Басқару сервері мен құрылғылар арасында арнаның ені.
- Басқару сервері және қашықтағы ішкі желілер арасындағы байланыс түрі және мұндай ішкі желілердің ішінде желілік арналардың сыйымдылығы.
- Қашықтағы құрылғыларда орналастырудың басында қауіпсіздік параметрлері қолданылады. Бұл параметрлер басқарылатын құрылғыға қашықтан қосылуға және орнатуды бастауға мүмкіндік береді.

Инсталляторлар параметрлерін конфигурациялау

Kaspersky бағдарламаларын желіге орналастыруға кіріспес бұрын, орнату параметрлерін – бағдарламаны орнату барысында конфигурацияланатын параметрлерді анықтап алу керек. Желілік агентті орнатқан кезде кем дегенде Басқару серверіне қосылу мекенжайын, мүмкін болса, кейбір қосымша параметрлерді белгілеу қажет. Таңдалған орнату тәсіліне байланысты, параметрлерді әртүрлі тәсілдермен белгілеуге болады. Қарапайым жағдайда (қолмен таңдалған құрылғыға интерактивті орнатқан кезде) қажетті параметрлерді инсталлятордың пайдаланушылық интерфейсі көмегімен белгілеуге болады.

Бұл параметрлерді конфигурациялау тәсілі құрылғылар топтарына бағдарламаларды тыныш орнатуға қолайсыз. Әдеттегі жағдайда әкімші орталықтандырылған түрде параметрлердің мәндерін көрсетуі тиіс, олар одан әрі желідегі таңдалған құрылғыларға тыныш орнату үшін қолданылуы мүмкін.

Орнату пакеттері

Қолданбаларды орнату параметрлерін конфигурациялаудың бірінші және негізгі тәсілі әмбебап болып табылады және қолданбаларды орнатудың барлық тәсілдеріне жарамды болып келеді: Kaspersky Security Center құралдарымен де, үшінші тарап құралдарының көпшілігі көмегімен де. Бұл тәсіл Kaspersky Security Center-де қолданбалардың орнату пакеттерін құруды білдіреді.

Орнату пакеттері келесі тәсілдермен жасалады:

- көрсетілген дистрибутивтерден, олардың құрамына кіретін *сипаттауыштар* негізінде автоматты түрде (орнату және нәтижені талдау ережелерін және басқа ақпаратты қамтитын kud кеңейтімі бар файлдар);

- инсталляторлардың немесе өзіндік пішімдегі инсталляторлардың орындалатын файлдарынан (.msi, .deb, .rpm) – стандартты немесе қолдау көрсетілетін қолданбалар үшін.

Жасалған орнату пакеттері ішкі қалталары мен файлдары салынған қалталар болып саналады. Бастапқы дистрибутивтен басқа, орнату пакеті өңделетін параметрлерді (инсталлятордың өзінің параметрлерін және орнатуды аяқтау үшін операциялық жүйені қайта іске қосу қажеттілігі сияқты жағдайларды өңдеу ережелерін қоса), сондай-ақ шағын көмекші модульдерді қамтиды.

Нақты қолдау көрсетілетін қолданба үшін ерекше инсталляция параметрлерінің мәндерін орнату пакетін жасаған кезде Басқару консолінің реттелмелі интерфейсінде белгілеуге болады. Kaspersky Security Center құралдарымен қолданбаларды қашықтан орнату жағдайында орнату пакеттері қолданбаның инсталляторын іске қосқан кезде оған әкімші белгілеген барлық параметрлер қолжетімді болатындай етіп құрылғыларға жеткізіледі. Kaspersky қолданбаларын орнатудың бөтен құралдарын қолданған кезде барлық орнату пакетінің, яғни дистрибутив пен оның параметрлерінің құрылғыдағы қолжетімділігін қамтамасыз ету жеткілікті. Орнату пакеттері Kaspersky Security Center ортақ қатынасы бар қалтаның сәйкес ішкі қалтасында жасалады және сақталады.

Орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетпеңіз.

Бөтен құралдармен оларды орналастырудың алдында Kaspersky қолданбалары үшін параметрлерді конфигурациялаудың осы тәсілін қалай қолдану керектігі туралы "Microsoft Windows топтық саясаттар механизмі көмегімен орналастыру" бөлімінде қараңыз.

Kaspersky Security Center орнатылғаннан кейін, бірден орнатуға дайын бірнеше орнату пакеттері, соның ішінде Microsoft Windows платформасына арналған Желілік агент пакеттері мен қауіпсіздік қолданбалары автоматты түрде жасалады.

Қолданбаға арналған лицензия үшін лицензиялық кілтті орнату пакетінің сипаттарында белгілеуге болатынына қарамастан, оқуға арналған орнату пакеттерінің орасан зор қолжетімділігі себебінен бұл лицензияларды тарату тәсілін қолданбаған жөн. Автоматты түрде таратылған лицензиялық кілттерді немесе лицензиялық кілттерді орнату тапсырмаларын қолданған жөн.

MSI сипаттары және түрлендіру файлдары

Windows платформасында орнату параметрлерін конфигурациялаудың тағы бір тәсілі, MSI және түрлендіру файлдарының сипаттарын белгілеу. Бұл тәсілді келесі жағдайларда пайдалануға болады:

- Microsoft штаттық құралдары немесе Windows топтық саясаттарымен жұмыс істеуге арналған басқа бөтен құрылғылар көмегімен Windows топтық саясаттары арқылы орнатқан кезде;

- Microsoft Installer пішімінде инсталляторлармен жұмысқа бағытталған бөтен құралдармен орнатқан кезде.

Қолданбаларды қашықтан орнатудың үшінші тарап құралдары арқылы орналастыру

Егер ұйымда қолданбаларды қашықтан орнатудың кез келген құралы болса (мысалы, Microsoft System Center), осы құралдардың көмегімен бастапқы орналастыруды жүзеге асырған жөн.

Келесі әрекеттерді орындау керек:

- Қолданылатын орналастыру құралы үшін ең қолайлы орнату параметрлерін конфигурациялау тәсілін таңдау.
- Басқару консолі интерфейсі арқылы орнату пакеттерінің параметрлерін өзгерту және осы орнату пакеттерінен қолданбаларды орналастырудың таңдалған үшінші тарап құралдарының жұмысы арасындағы синхрондау механизмін анықтау.
- Ортақ қатынасы бар қалтадан орнатылған жағдайда, осы файл ресурсының жеткілікті өнімділігіне көз жеткізіңіз.

Kaspersky Security Center бағдарламаларын қашықтан орнату тапсырмалары туралы

Kaspersky Security Center қолданбаларды қашықтан орнату тапсырмалары түрінде іске асырылған қолданбаларды қашықтан орнатудың әртүрлі механизмдерін ұсынады (күшпен орнату, қатты дисктің үлгісін көшіру арқылы орнату, Microsoft Windows топтық саясаттары көмегімен орнату). Қашықтан орнату тапсырмасын көрсетілген басқару тобы үшін де, арнайы құрылғылар немесе құрылғыны таңдау үшін де жасауға болады (мұндай тапсырмалар **Тапсырмалар** қалтасында Басқару консолінде көрсетіледі). Тапсырманы жасау кезінде, сіз осы тапсырманы пайдаланып, орнатылатын орнату пакеттерін (Желілік агент және/немесе басқа қолданба) таңдай аласыз, сонымен қатар қашықтан орнату тәсілін анықтайтын бірқатар параметрлерді орната аласыз. Сонымен қатар, қолданбаларды қашықтан орнату шеберін қолдануға болады, оның негізінде қолданбаларды қашықтан орнату тапсырмасын жасау және нәтижелерді мониторингтеу жатыр.

Басқару топтарына арналған тапсырмалар тек осы топқа жататын құрылғыларда ғана емес, таңдалған топтың барлық ішкі топтарының барлық құрылғыларында да жұмыс істейді. Егер тапсырма параметрлерінде тиісті параметр қосылса, тапсырма осы топта немесе оның ішкі топтарында орналасқан қосалқы Басқару серверлерінің құрылғыларына қолданылады.

Құрылғылар жиынтығына арналған тапсырмалар, тапсырманы іске қосу кезінде құрылғыларды таңдау құрамына сәйкес әрбір рет іске қосу кезінде клиент құрылғыларының тізімін жаңартады. Егер құрылғыларды таңдауда қосалқы Басқару серверлеріне қосылған құрылғылар болса, тапсырма осы құрылғыларда да іске қосылады. Бұл параметрлер және орнату тәсілдері туралы толығырақ осы бөлімде кейін айтылады.

Қосалқы Басқару серверіне қосылған құрылғыларда қашықтан орнату тапсырмасының сәтті жұмысы үшін ауыстыру тапсырмасымен сәйкес қосалқы Басқару серверлеріне тапсырма қолданатын орнату пакеттерін алдын ала ауыстыру керек.

Құрылғының бейнесін қармау және көшіру арқылы енгізу

Егер операциялық жүйені және басқа бағдарламалық жасақтаманы орнату (немесе қайта орнату) жүргізілетін құрылғыларға Желілік агентті орнату керек болса, құрылғының үлгісін қармау және көшіру механизмін қолдануға болады.

Қатты дискті қармау және көшіру арқылы орналастыруды орындау үшін:

1. Желілік агентті және қауіпсіздік бағдарламасын қоса, орнатылған операциялық жүйемен және жұмысқа қажетті бағдарламалық жасақтаманың жиынтығымен эталондық құрылғыны жасау.

2. "Эталондық" құрылғының үлгісін қармау және одан әрі бұл үлгіні Kaspersky Security Center тапсырмасы арқылы жаңа құрылғыларға тарату.

   Диск үлгілерін қармау және орнату үшін ұйымдағы бөтен құралдарды да, Kaspersky Security Center ұсынатын функционалдылықты да (Осалдықтар мен патчтарды басқаруға лицензия бар болса) пайдалануға болады.

Егер диск үлгілерімен жұмыс істеу үшін бөтен құралдар қолданылса, құрылғыға эталондық үлгіден орналастырған кезде Kaspersky Security Center басқарылатын құрылғыны сәйкестендіретін ақпаратты жоюды қамтамасыз ету керек. Керісінше жағдайда Басқару сервері одан әрі бірдей үлгіні көшіру жолымен жасалған құрылғыларды дұрыс ажырата алмайды.

Kaspersky Security Center құралдарымен диск үлгісін қармау кезінде бұл мәселе автоматты түрде шешіледі.

Бөтен құралдармен қатты дисктің үлгісін көшіру

Желілік агенті орнатылған құрылғы үлгісін қармау үшін бөтен құралдарды қолданған кезде келесі әдістердің бірінші қолдану керек:

- Ұсынылған әдіс. Желілік агентті анықтамалық құрылғыға орнатқан кезде, желілік агент қызметінің бірінші іске қосылуының алдында құрылғы кескінін түсіріңіз (себебі құрылғыны анықтайтын бірегей ақпарат желілік агентті басқару серверіне бірінші рет қосқан кезде жасалады). Одан әрі тіпті үлгіні қармау операциясын орындауға дейін Желілік агенттің қызметін іске қосуға жол бермеу ұсынылады.

- Эталондық құрылғыда Желілік агенттің қызметін тоқтатыңыз және dupfix кілтімен klmover утилитасын іске қосыңыз. klmover утилитасы Желілік агенттің орнату пакетінің құрамына кіреді. Одан әрі тіпті үлгіні қармау операциясын орындауға дейін Желілік агенттің қызметін іске қосуға жол бермеңіз.

- Үлгіні орналастырғаннан кейін операциялық жүйені бірінші іске қосқан кезде құрылғыларда Желілік агенттің қызметін бірінші іске қосуға дейін -dupfix кілтімен klmover утилитасын іске қосуды қамтамасыз ету міндетті. klmover утилитасы Желілік агенттің орнату пакетінің құрамына кіреді.

- Желілік агенттің дискісін клондау режимін пайдалану.

Егер қатты диск үлгісі қате көшірілсе, сіз бұл мәселені шеше аласыз.

Сондай-ақ, Желілік агент орнатылмай-ақ құрылғы кескінін түсіруге болады. Бұл әрекетті орындау үшін кескінді мақсатты құрылғыларға орналастырып, одан кейін Желілік агентті орнатыңыз. Бұл әдісті пайдаланған кезде құрылғыдан автономды орнату пакеттері бар желілік қалтаға кіруді беріңіз.

Қатты дискінің кескіні дұрыс көшірілмеді

Желілік агент орнатылған қатты диск кескінінің көшірмесі орналастыру ережелерін ескермей орындалса, Басқару консоліндегі кейбір құрылғылар атын үнемі өзгертетін жалғыз құрылғы белгішесі ретінде көрсетілуі мүмкін.

Бұл мәселені шешу үшін келесі әдістерді қолдануға болады:

- Желілік агентті жою.

  Бұл тәсіл ең сенімді болып табылады. Кескіннен қате көшірілген құрылғыларда үшінші тарап құралдарын пайдаланып Желілік агент бағдарламасын жойып, оны қайта орнату керек. Желілік агентті Kaspersky Security Center арқылы жою мүмкін емес, себебі барлық ақаулы құрылғыларды Басқару сервері үшін ажыратуға болмайды (олардың барлығында Басқару консолінде бірдей белгіше бар).

- «-dupfix» кілті арқылы klmover утилитасын іске қосу.

  Проблемалық құрылғыларда (кескіннен қате көшірілген барлық құрылғыларда) klmover утилитасын Желілік агент орнату қалтасында орналасқан "-dupfix" пернесі (klmover -dupfix) арқылы бір рет іске қосу үшін үшінші тарап құралдарын пайдалану керек. Утилитаны Kaspersky Security Center құралдары арқылы іске қосу мүмкін емес, себебі барлық проблемалы құрылғылар Басқару сервері үшін ажыратылмайды (олардың барлығында Басқару консолінде бірдей белгіше бар).

  Содан кейін, қызметтік бағдарламаны іске қоспас бұрын ақаулық құрылғылар көрсетілген белгішені жою керек.

- Қате көшірілген құрылғыларды анықтау ережесін қатаңдату.

  > Бұл тәсілді Басқару сервері және 10 Service Pack 1 немесе одан кейінгі нұсқасының Желілік агенттері орнатылған жағдайда ғана пайдалануға болады.

  Қате көшірілген Желілік агенттерді анықтау ережесін құрылғының NetBIOS атауын өзгерту осындай Желілік агенттерді автоматты түрде «жөндеуге» әкелетіндей күшейту керек (көшірілген құрылғыларда әртүрлі NetBIOS атаулары бар деп болжанады).

  Басқару сервері бар құрылғыда тізілімге келесі .reg файлын импорттаңыз және Басқару сервері қызметін қайта іске қосыңыз.

  - Басқару сервері бар құрылғыда 32 разрядтық операциялық жүйе орнатылған болса:

  ```
  REGEDIT4
  [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
  "KLSRV_CheckClones"=dword:00000003
  ```

  - Басқару сервері бар құрылғыда 64 разрядтық операциялық жүйе орнатылған болса:

  ```
  REGEDIT4
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
  "KLSRV_CheckClones"=dword:00000003
  ```

Microsoft Windows топтық саясаттары тетігінің көмегімен орналастыру

Желілік агенттерді бастапқы орналастыруды, келесі шарттарды орындаған кезде Microsoft Windows топтық саясаттарының көмегімен жүзеге асырылған жөн:

- құрылғылар Active Directory доменінің мүшелері;

- орналастыру жоспары, Желілік агенттерді орналастыра бастауға дейін құрылғылардың штаттық жағдайда қайта іске қосылуын күте тұруға мүмкіндік береді немесе құрылғыларға Windows топтық саясатын күшпен қолдануға болады.

Осы орналастыру тәсілінің мәні келесіде:

- Microsoft Installer пішіміндегі қолданбаның дистрибутив бумасы (MSI пакеті) ортақ қатынасы бар қалтада орналастырылады (құрылғылардың LocalSystem есептік жазбалары оқуға қатынасу мүмкіндігі бар қалтада).
- Active Directory топтық саясатында осы дистрибутивті орнату нысаны жасалады.
- Орнатудың әрекет ету ауқымы ұйымдық бөлімшеге және/немесе құрылғыларды қамтитын қауіпсіздік тобына байлау арқылы белгіленеді.
- Құрылғының доменге кезекті кіруі кезінде (жүйеге құрылғы пайдаланушылар кіргенге дейін) орнатылған қолданбалар арасында қажетті қолданбаның болуын тексеру орындалады. Қолданба болмаса, дистрибутив саясатта белгіленген ресурстан жүктеп алынып, орнатылады.

Осы орналастыру тәсілінің артықшылықтарының бірі, тағайындалған қолданбалар, пайдаланушы жүйеге кірмес бұрын, операциялық жүйені жүктеу кезінде құрылғыларға орнатылады. Тіпті қажетті құқықтары бар пайдаланушы қолданбаны жойса да, операциялық жүйені келесі жолы жүктеу кезінде, ол қайтадан орнатылады. Осы орналастыру тәсілінің кемшілігі, әкімші тарапынан топтық саясатта жүзеге асырылған өзгерістер құрылғыны қайта іске қоспайынша күшіне енбейді (қосымша құралдарды қолданбай).

Топтық саясаттардың көмегімен, Желілік агентті де, инсталляторлары Windows Installer пішіміне ие басқа қолданбаларды да орнатуға болады.

Осы орналастыру тәсілін таңдау кезінде, бұдан бөлек, Windows топтық саясатын қолдану кезінде құрылғыға файлдар көшірілетін файлдық ресурсқа түсетін жүктемені бағалау керек.

Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасының көмегімен Microsoft Windows саясаттарымен жұмыс істеу

Microsoft Windows топтық саясаттарымен бағдарламаларды орнатудың ең қарапайым тәсілі - Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасының сипаттарында **Active Directory топтық саясаттарында бума орнатуды тағайындау** параметрін таңдау. Бұл жағдайда тапсырманы іске қосқан кезде Басқару сервері келесі әрекеттерді орындайды:

- Microsoft Windows топтық саясатында қажетті нысандарды жасайды.
- Құрылғыларды қосатын және осы қауіпсіздік топтары үшін таңдалған қолданбаларды орнатуды тағайындайтын арнайы қауіпсіздік топтарын жасайды. Қауіпсіздік тобының құрамы тапсырманы іске қосқан сәтте арнайы құрылғыларға сәйкес өзектендіріледі.

Бұл функцияның жұмысқа қабілетін қамтамасыз ету үшін тапсырма параметрлерінде Active Directory топтық саясаттарын түзетуге құқықтары бар есептік жазбаны көрсету керек.

Егер бір тапсырмамен Желілік агентті және басқа қолданбаны орнату болжамданса, **Active Directory топтық саясаттарында бума орнатуды тағайындау** параметрін таңдау Active Directory саясатында тек қана Желілік агент үшін орнату нысанын жасауға әкеледі. Тапсырмада екінші таңдалған қолданба ол құрылғыға орнатылғаннан кейін Желілік агенттің құралдарымен орнатылады. Егер қандай да бір себеппен Желілік агенттен ерекшеленетін қолданбаны дәл Windows топтық саясаттары көмегімен орнату қажет болса, онда осы орнату пакеті үшін орнату тапсырмасын жасау қажет (Желілік агенттің пакеті жоқ). Microsoft Windows топтық саясаттары көмегімен барлық қолданбаларды орнатуға болмайды. Мұндай мүмкіндік туралы қолданбаны орнату тәсілдері туралы ақпаратқа жүгініп біле аласыз.

Егер қажетті нысандар топтық саясатта Kaspersky Security Center құралдарымен жасалса, орнату пакеті ретінде Kaspersky Security Center ортақ қатынасы бар қалта қолданылады. Орналастыруды жоспарлаған кезде осы қалтадағы оқу жылдамдығын құрылғылар санымен және орнатылатын дистрибутивтің өлшемімен салыстыру керек. Kaspersky Security Center ортақ қатынасы бар қалтасын қуатты мамандандырылған файлдық қоймаға орналастырған жөн.

Қарапайымдылығымен қатар, Kaspersky Security Center құралдарымен Windows топтық саясаттарын автоматты түрде жасау тағы бір артықшылыққа ие: Желілік агентті орнатуды жоспарлаған кезде орнатуды аяқтағаннан кейін құрылғылар автоматты түрде жылжытылатын Kaspersky Security Center басқару тобын көрсету оңай. Топты жаңа тапсырма жасау шеберінде немесе қашықтан орнату тапсырмаларының параметрлерінде көрсетуге болады.

Kaspersky Security Center құралдарымен Windows топтық саясаттарымен жұмыс істеген кезде топтық саясат нысаны үшін құрылғыларды белгілеу қауіпсіздік тобын жасау жолымен жүргізіледі. Kaspersky Security Center қауіпсіздік тобының құрамын ағымдағы тапсырманың арнайы құрылғыларымен синхрондайды. Топтық саясаттармен жұмыс істеу үшін басқа құралдарды қолданған кезде топтық саясаттардың нысандарын тікелей Active Directory таңдалған бөлімшелеріне байлауға болады.

Қолданбаларды Microsoft Windows саясаттары көмегімен өз бетінше орнату

Әкімші Windows топтық саясатында орнату үшін қажетті нысандарды өз бетінше жасай алады. Бұл жағдайда Kaspersky Security Center ортақ қатынасы бар қалтада жатқан пакеттерге сілтеме жасауға немесе пакеттерді бөлек файл серверіне салуға және оларға сілтеме жасауға болады.

Келесі орнату сценарийлері жүзеге асырылуы мүмкін:

- Әкімші орнату пакетін жасап, оның сипаттарын Басқару консолінде конфигурациялайды. Топтық саясат нысаны Kaspersky Security Center ортақ қатынасы бар қалтада жатқан осы конфигурацияланған пакеттің MSI-файлына сілтеме жасайды.

- Әкімші орнату пакетін жасап, оның сипаттарын Басқару консолінде конфигурациялайды. Содан соң, әкімші осы пакеттің EXEC ішкі қалтасын Kaspersky Security Center ортақ қатынасы бар қалтасынан ұйымның мамандандырылған файл ресурсындағы қалтаға толығымен көшіріп алады. Топтық саясат нысаны, ұйымның мамандандырылған файл ресурсындағы ішкі қалтада жатқан осы пакеттің MSI файлына сілтеме жасайды.

- Әкімші интернеттен қолданбаның дистрибутивін (оның ішінде Желілік агенттің дистрибутивін) жүктеп алады және оны ұйымның мамандандырылған файл ресурсына жүктейді. Топтық саясат нысаны, ұйымның мамандандырылған файл ресурсындағы ішкі қалтада жатқан осы пакеттің MSI файлына сілтеме жасайды. Орнату параметрлерін конфигурациялау MSI сипаттарын конфигурациялау немесе MST түрлендіру файлдарын конфигурациялау арқылы жүзеге асырылады.

Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру

Желілік агентті немесе басқа бағдарламаларды бастапқы енгізу үшін әрбір құрылғыда жергілікті әкімші құқықтары бар пайдаланушы есептік жазбалары болған жағдайда, Kaspersky Security Center қашықтан орнату тапсырмасымен таңдалған орнату пакеттерін мәжбүрлі түрде орнатуға болады.

Күшпен орнату құрылғылар тікелей Басқару серверіне қолжетімді болмаған жағдайда қолданылуы мүмкін: мысалы, құрылғылар оқшауланған желілерде орналасқан немесе құрылғылар жергілікті желіде, ал Басқару сервері – демилитаризацияланған аймақта орналасқан.

Бастапқы енгізу кезінде желілік агент орнатылмайды. Сондықтан қашықтан орнату тапсырмасының параметрлерінде Желілік агент көмегімен қолданбаны орнату үшін қажетті файлдарды таратуды таңдау мүмкін емес. Файлдарды басқару сервері немесе тарату нүктесі көмегімен операциялық жүйе ресурстарын пайдаланып қана тарата аласыз.

Басқару серверінің қызметі мақсатты құрылғыларда әкімші құқықтары бар есептік жазбамен іске қосылуы керек. Сондай-ақ қашықтан орнату тапсырмасы параметрлерінде admin$ жалпы қатынасы бар әкімшілік ресурстарына кіре алатын есептік жазбаны көрсетуге болады.

Әдепкісінше қашықтан орнату тапсырмасы құрылғыларға басқару сервері іске қосылған есептік жазбаның тіркелгі деректері көмегімен қосылады. Бұл қашықтан орнату тапсырмасы орындалатын есептік жазба емес, admin$ жалпы қатынасы бар әкімшілік ресурстарына кіру үшін қолданылатын есептік жазба екенін ескеріңіз. Орнату LocalSystem есептік жазбасында орындалады.

Мақсатты құрылғыларды олар тиесілі Kaspersky Security Center басқару тобын таңдау немесе белгілі бір шартқа негізделген құрылғылар таңдауын жасау арқылы анық (тізімде) көрсетуге болады. Орнатуды іске қосу уақыты тапсырма кестесімен анықталады. Тапсырманың сипаттарында **Өткізіп алынған тапсырмаларды іске қосу** параметрі қосулы болса, тапсырма құрылғыларды қосу кезінде немесе оларды мақсатты басқару тобына көшіру кезінде бірден іске қосылуы мүмкін.

Мәжбүрлеп орнату әрекеті, орнату пакеттерін мақсатты құрылғыларға жеткізу, содан соң файлдарды құрылғылардың әрқайсысының admin$ басқару ресурсына көшіру және оларға көмекші қызметтерді қашықтан тіркеу арқылы жүзеге асырылады. Орнату пакеттерін мақсатты құрылғыларға жеткізу әрекеті, желілік өзара әрекеттесуге жауап беретін Kaspersky Security Center функциясы арқылы жүзеге асырылады. Бұл жағдайда, келесі шарттар орындалуы керек:

- Мақсатты құрылғыларға басқару серверінен немесе тарату нүктесінен қол жеткізуге болады.
- Желіде құрылғыларға арналған атаулар рұқсаты дұрыс жұмыс істеп жатыр.
- Мақсатты құрылғыларда admin$ жалпы қатынасын басқару ресурстары қосулы.
- Мақсатты құрылғыларда келесі жүйелік қызметтер іске қосылған:
  - Сервер (LanmanServer).

    Әдепкі бойынша бұл қызмет іске қосылған.
  - DCOM Server Process Launcher (DcomLaunch).
  - RPC Endpoint Mapper (RpcEptMapper).
  - Қашықтағы процедураны шақыру (Remote Procedure Call, RpcSs).
- TCP 445 порты Windows басқару құралдары көмегімен қашықтан қол жеткізуге рұқсат беру үшін мақсатты құрылғыларда ашық.

  Сондай-ақ, қашықтан орнатуды орындамас бұрын (егер UDP 137 қолжетімді болмаса) мақсатты құрылғының операциялық жүйе түрін анықтау үшін TCP 445 порты тексеріледі.

  TCP 139, UDP 137 және UDP 138 ескі протоколдармен пайдаланылады және енді ағымдағы бағдарламаларға қажет емес.

  Басқару серверін және тарату нүктелерін мақсатты құрылғыларға қосу үшін желілік экранда динамикалық шығыс кіру порттарына рұқсат берілуі керек.

- Желілік агентті енгізу кезінде Active Directory домен саясатының қауіпсіздік параметрлерінде NTLM протоколының жұмысын қамтамасыз етуге рұқсат берілді.
- Microsoft Windows XP басқаратын мақсатты құрылғыларда Simple File Sharing режимі өшірулі.
- Мақсатты құрылғыларда *классикалық бөлісу және қауіпсіздік моделінің параметрлері орнатылған — жергілікті пайдаланушылар өздерін аутентификациялайды.* Мұндай модель *тек қонақ болуы мүмкін емес – жергілікті пайдаланушылар қонақ ретінде аутентификациялайды.*
- Құрылғылар домен мүшелері болып табылады немесе құрылғыларда басқару құқықтары бар бірегейлендірілген есептік жазбалар алдын ала жасалған.

Windows Server 2003 немесе одан жоғары операциялық жүйе нұсқасы орнатылған Active Directory доменіне қосылмаған құрылғыда желілік агент немесе басқа бағдарламаларды сәтті енгізу үшін сол құрылғыда қашықтағы UAC өшіру керек. Қашықтағы UAC — жергілікті әкімші есептік жазбаларының admin$-ке қол жеткізе алмауы себептерінің бірі, бұл желілік агентті және басқа бағдарламаларды мәжбүрлі түрде енгізу үшін қажет. Қашықтағы UAC өшіру жергілікті UAC-ге әсер етпейді.

Kaspersky Security Center басқару топтарында әлі орналастырылмаған жаңа құрылғыларға орнатқан кезде, қашықтан орнату тапсырмасының сипаттарында Желілік агентті орнату аяқталғаннан кейін құрылғылар көшірілетін басқару тобын белгілеуге болады.

Топтық тапсырманы жасау кезінде, топтық тапсырма таңдалған топтың барлық салынған ішкі топтарының құрылғыларына әсер ететінін есте ұстаған жөн. Сондықтан, орнату тапсырмаларын ішкі топтарда қайталамау керек.

Бағдарламаларды мәжбүрлі түрде орнату үшін тапсырмаларды жасаудың жеңіл жолы — автоматты түрде орнату. Ол үшін басқару тобының сипаттарында орнату пакеттерінің тізімін ашып, осы топтың құрылғыларына орнатылуы керек пакеттерді таңдау керек. Нәтижесінде, осы топтың және оның ішкі топтарының барлық құрылғыларында, таңдалған орнату пакеттері автоматты түрде орнатылады. Пакеттер орнатылатын кезең, желінің өткізу қабілетіне және желідегі құрылғылардың жалпы санына байланысты.

Орнату пакеттерін мақсатты құрылғыларға тарату кезінде басқару серверіндегі жүктемені азайту үшін орнату тапсырмасында тарату нүктелерін пайдаланып, орнатуды таңдауға болады. Орнатудың бұл тәсілі, тарату нүктелерімен тағайындалған құрылғыларға елеулі жүктеме түсіретінін ескеру қажет. Тарату нүктелеріне қойылатын талаптарға сай құрылғыларды таңдау ұсынылады. Тарату нүктелерін пайдалансаңыз, олардың мақсатты құрылғыларды орналастыратын оқшауланған ішкі желілердің әрқайсысында болуын қамтамасыз ету керек.

Жергілікті орнату орталықтары ретінде тарату нүктелерін қолдану ішкі желі ішінде құрылғылар арасында кең байланыс арнасы бар болған кезде тар байланыс арнасымен Басқару серверіне қосылған ішкі желілерде құрылғыларға орнату үшін де ыңғайлы болуы мүмкін.

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit қалтасы бар бөлімде бос орын көлемі орнатылатын бағдарламалар дистрибутивтерінің жиынтық көлемінен бірнеше есе асып кетуі қажет.

Kaspersky Security Center қалыптастырған автономды пакеттерді іске қосу

Желілік агент пен қолданбаларды бастапқы орналастырудың жоғарыда сипатталған тәсілдері барлық қажетті шарттарды орындай алмағандықтан, жүзеге аса бермеуі мүмкін. Мұндай жағдайларда, Kaspersky Security Center құралдарымен орнатудың қажетті параметрлері бар әкімші дайындаған орнату пакеттерінен *жеке орнату пакеті* деп аталатын бірыңғай орындалатын файл жасауға болады. Автономды орнату пакеті Kaspersky Security Center ортақ қатынасы бар қалтаға орналастырылады.

Kaspersky Security Center бағдарламасының көмегімен, таңдалған пайдаланушыларға ортақ қатынасы бар қалтадағы осы файлға сілтемені электрондық пошта арқылы (интерактивті түрде немесе "тыныш" орнату "-s" кілтімен) файлды іске қосу туралы өтінішпен бірге таратуға болады. Автономды орнату пакетін Kaspersky Security Center ортақ қатынасы бар қалтаға қатынасы жоқ құрылғы пайдаланушылары үшін электрондық пошта хабарға бекітуге болады. Әкімші автономды пакетті алынбалы дискке көшіре алады және пакетті кейін іске қосу мақсатымен қажетті құрылғыға жеткізе алады.

Автономды пакетті Желілік агент пакетінен, басқа қолданба пакетінен (мысалы, қауіпсіздік бағдарламасынан) немесе бірден екі пакеттен де жасауға болады. Егер автономды пакет Желілік агент пен басқа қолданбадан жасалса, онда орнату Желілік агенттен басталады.

Желілік агентпен автономды пакетті жасау кезінде, Желілік агентті орнату аяқталғаннан кейін жаңа құрылғылар (бұрын басқару топтарында орналастырылмаған) автоматты түрде көшірілетін басқару тобын көрсетуге болады.

Автономды пакеттер интерактивті түрде (әдепкі бойынша), оларға кіретін қолданбаларды орнату нәтижесін көрсете отырып немесе "тыныш" режимде ("-s" кілтімен іске қосылғанда) жұмыс істей алады. "Тыныш" режимді кез келген скрипттерден орнату үшін пайдалануға болады (мысалы, операциялық жүйенің кескінін орналастыру аяқталғаннан кейін іске қосылатын скрипттерден және т.с.с.). "Тыныш" режимде орнату нәтижесі процесті қайтару кодымен анықталады.

Linux жүйесіне арналған автономды желі агентінде nmap утилитасындағы қосымша тәуелділік бар. nmap утилитасы болмаса немесе 6.0 нұсқасынан ертерек болса, Broadcast DHCP Discover функциясына қолдау көрсетілмейді.

Қолданбаларды қолмен басқару мүмкіндіктері

Әкімшілер немесе тәжірибелі пайдаланушылар қолданбаларды интерактивті режимде қолмен орната алады. Бұл арада, сіз Kaspersky Security Center ортақ қатынасы бар қалтасында орналасқан бастапқы дистрибутивтерді де, олардан құрылған орнату пакеттерін де пайдалана аласыз. Инсталляторлар әдепкі бойынша интерактивті режимде жұмыс істейді, пайдаланушыдан барлық қажетті параметр мәндерін сұрайды. Бірақ "-s" кілті бар орнату пакетінің түбірінен setup.exe процесін іске қосқан кезде, инсталлятор орнату пакетін реттеген кезде белгіленген параметрлермен "тыныш" режимде жұмыс істейді.

Kaspersky Security Center ортақ қатынасы бар қалтасында орналасқан орнату пакетінің түбірінен setup.exe іске қосылған кезде, алдымен пакет уақытша жергілікті қалтаға көшіріледі, содан кейін қолданба инсталляторы жергілікті қалтадан іске қосылады.

MST файлын құру

MSI пакетінің мазмұнын түрлендіру және бар MSI файлына теңшелетін параметрлерді қолдану үшін MST пішімінде түрлендіру файлын жасау керек. Ол үшін Windows SDK құрамына кіретін Orca.exe редакторын пайдаланыңыз.

MST файлын жасау үшін:

1. Orca.exe редакторын іске қосыңыз.
2. **Файл** қойындысына өтіп, мәзірден **Ашу** түймесін басыңыз.
3. Kaspersky Network Agent.msi файлын таңдаңыз.

4. **Түрлендіру** қойындысына өтіп, мәзірден **Жаңа түрлендіру** тармағын таңдаңыз.

5. **Кестелер** бағанында **Сипатты** таңдап, келесі мәндерді көрсетіңіз:

   - *EULA=1*
   - *SERVERADDRESS=<Басқару сервері мекенжайы>*

   Сақтау түймесін басыңыз.

6. **Түрлендіру** қойындысына өтіп, мәзірден **Түрлендіруді жасау** пәрменін таңдаңыз.

7. Ашылған терезеде құрылатын түрлендіру файлының атын көрсетіңіз және **Сақтау** түймесін басыңыз.

MST файлы сақталды.

Желілік агенті орнатылған құрылғыларға бағдарламаларды қашықтан орнату

Егер құрылғыда негізгі Басқару серверіне немесе оның қосалқы Серверлерінің біріне қосылған жұмысқа жарамды Желілік агент орнатылған болса, онда осы құрылғыда Желілік агенттің нұсқасын жаңартуға, сондай-ақ Желілік агенттің көмегімен кез келген қолдау көрсетілетін қолданбаларды орнатуға, жаңартуға немесе жоюға болады.

Бұл функция, қолданбаларды қашықтан орнату тапсырмасының сипаттарында **Желілік агенттің көмегімен** параметрі тарапынан қосылады.

Параметр таңдалған болса, құрылғыларға әкімші белгілеген орнату параметрлері бар орнату пакеттерін жіберу, Желілік агент пен Басқару сервері арасындағы байланыс арналары арқылы жүзеге асырылады.

Басқару серверіне түсетін жүктемені оңтайландыру және Басқару сервері мен құрылғылар арасындағы трафикті азайту үшін, әрбір қашықтағы желіде немесе әрбір кеңінен таратылатын доменде тарату нүктелерін тағайындаған жөн ("Тарату нүктелері туралы" және "Басқару топтары құрылымын құру және тарату нүктелерін тағайындау" бөлімдерін қараңыз). Бұл жағдайда, орнату пакеттері мен инсталлятор параметрлерін тарату, құрылғыларға Басқару серверінен тарату нүктелері арқылы жүзеге асырылады.

Сондай-ақ, тарату нүктелерін қолдана отырып, бағдарламаларды орналастыру барысында желілік трафикті бірнеше есе төмендетуге мүмкіндік беретін орнату пакеттерін кеңінен (көп мекенжайға) таратуға болады.

Орнату пакеттерін құрылғыларға Желілік агенттер мен Басқару сервері арқылы байланыс арналары бойынша жіберу кезінде, жіберуге дайындалған орнату пакеттері %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\adminkit\1093\.working\FTServer қалтасында қосымша түрде кэштеледі. Үлкен өлшемдегі әртүрлі орнату пакеттерінің көп бөлігін қолдану кезінде және тарату нүктелерінің көп санында осы қалтаның өлшемі айтарлықтай ұлғаюы мүмкін.

FTServer қалтасындағы файлдарды жоюға болмайды. Бастапқы орнату пакеттерін жою кезінде, тиісті деректер FTServer қалтасынан да автоматты түрде жойылатын болады.

Тарату нүктелері тарапынан қабылданатын деректер %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp қалтасында сақталады.

$FTCITmp қалтасындағы файлдарды жоюға болмайды. Қалтадағы деректерді қолданатын тапсырмаларды аяқтау шамасына қарай, осы қалтаның ішіндегісі автоматты түрде жойылады.

Орнату пакеттері, желі арқылы беру үшін оңтайландырылған аралық қоймадан Басқару сервері мен Желілік агент арасындағы байланыс арналары бойынша таратылатындықтан, орнату пакетінің бастапқы қалтасындағы орнату пакеттеріне өзгеріс енгізуге болмайды. Мұндай өзгерістерді Басқару сервері автоматты түрде ескермейді. Орнату пакеттерінің файлдарын қолмен өзгерту қажет болса (мұны жасау ұсынылмайды), Басқару консоліндегі орнату пакетінің қандай да бір параметрлерін міндетті түрде өзгерту керек. Басқару консоліндегі орнату пакетінің параметрлерін өзгерту, Басқару серверін құрылғыға жіберуге дайындалған кештегі пакет кескінін жаңартуға мәжбүрлейді.

Қашықтан орнату тапсырмасында құрылғыларды қайта жүктеуді басқару

Жиі қолданбаларды қашықтан орнатуды аяқтау үшін (әсіресе Windows платформасында) құрылғыны қайта іске қосу қажет.

Егер Kaspersky Security Center бағдарламаларды қашықтан орнату тапсырмасы қолданылса, жаңа тапсырма жасау шеберінде немесе жасалған тапсырма сипаттарының терезесінде (**Операциялық жүйені қайта іске қосу** бөлімі) Windows операциялық жүйесі бар құрылғыны қайта іске қосу қажеттілігінде әрекеттің нұсқасын таңдауға болады:

- **Құрылғыны қайта іске қоспау**. Бұл жағдайда автоматты қайта іске қосу орындалмайды. Орнатуды аяқтау үшін құрылғыны қайта іске қосу керек (мысалы, қолмен немесе құрылғыларды басқару тапсырмасы көмегімен). Қайта іске қосу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа серверлерге және үздіксіз жұмыс критикалық түрде маңызды басқа құрылғыларға орнату тапсырмалары үшін қолайлы.

- **Құрылғыны қайта іске қосу**. Бұл жағдайда, егер қайта іске қосу орнатуды аяқтау үшін қажет болса, қайта іске қосу автоматты түрде орындалады. Бұл нұсқа жұмыста мерзімді үзілістерге жол берілетін (сөндіру, қайта іске қосу) құрылғыларға арналған орнату тапсырмаларына қолайлы.

- **Пайдаланушыдан әрекетті орындауды сұрау**. Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). **Пайдаланушыдан әрекетті орындауды сұрау** нұсқасы пайдаланушылары қайта іске қосу үшін анағұрлым қолайлы сәтті таңдау мүмкіндігіне ие болуы тиіс жұмыс станцияларына анағұрлым қолайлы.

Қауіпсіздік бағдарламасының орнату пакетіндегі дерекқорларды жаңартудың орындылығы

Орналастыру алдында, қауіпсіздік бағдарламасының дистрибутивімен бірге таратылатын антивирустық дерекқорларды (автопатч модульдерін қоса) жаңарту мүмкіндігін ескеру қажет. Орналастыруды бастамас бұрын қолданбаның орнату пакетінің құрамындағы дерекқорларды мәжбүрлеп жаңартқан жөн (мысалы, таңдалған орнату пакетінің мәнмәтіндік мәзіріндегі тиісті пәрменді қолдану арқылы). Бұл құрылғыларда қорғанысты орналастыруды аяқтау үшін қажет қайта жүктеу санын азайтады.

Ерікті орындалатын файлдардың басқарылатын құрылғыларында іске қосу үшін Kaspersky Security Center қолданбаларын қашықтан орнату құралдарын қолдану

Орнату пакетін жасау шеберінің көмегімен, ерікті орындалатын файлды таңдауға және ол үшін пәрмен жолының параметрлерін белгілеуге болады. Бұл арада, орнату пакетіне таңдалған файлдың өзін де, осы файл орналасқан қалтаның барлығын да салып қоюға болады. Содан кейін, қашықтан орнату тапсырмасын жасап, жасалған орнату пакетін таңдау керек.

Тапсырманың жұмыс барысында, құрылғыларда жасау кезінде көрсетілген, пәрмен жолының параметрлері белгіленген орындалатын файл іске қосылады.

Microsoft Windows Installer (MSI) пішіміндегі инсталляторлар қолданылса, Kaspersky Security Center бағдарламасы орнату нәтижесін талдау бойынша штаттық мүмкіндіктерді қолданады.

Осалдықтар мен патчтарды басқаруға арналған лицензия, корпоративтік ортада кеңінен таралған қолдау көрсетілетін қолданбалардың бірі үшін орнату пакетін жасау кезінде, Kaspersky Security Center бағдарламасы өзінің жаңартылатын дерекқорындағы орнату нәтижелерін талдау және орнату ережелерін де қолданады.

Өзге жағдайларда, орындалатын файлдар үшін әдепкі бойынша іске қосылған процестің және ол іске қосқан еншілес процестердің барлығының аяқталғанын күту керек. Іске қосылған процестер аяқталған кезде, тапсырма бастапқы процесті қайтару кодына қарамастан сәтті аяқталады. Тапсырманың осындай жүріс-тұрысын өзгерту үшін, тапсырманың жасау алдында, жасалған орнату пакетінің қалтасы мен оның ішкі қалталарында Kaspersky Security Center жасаған kpd кеңейтімі бар файлдарды қолмен өзгерту керек.

.kpd файлдары ASCII кодтауын пайдаланады. .kud файлдары Юникод кодтауын пайдаланады.

Тапсырма іске қосылған процестің аяқталуын күтпеуі үшін, [SetupProcessResult] секциясында Wait параметрі үшін 0 мәнін белгілеу керек:

```
[SetupProcessResult]
Wait=0
```

Windows платформасында тапсырма өзі іске қосқан еншілес процестердің емес, бастапқы процестің аяқталуын ғана күтуі үшін, онда [SetupProcessResult] секциясында WaitJob параметрі үшін 0 мәнін белгілеу керек, мысалы:

```
[SetupProcessResult]
WaitJob=0
```

Жүріп жатқан процестің қайтару кодына байланысты тапсырма сәтті аяқталуы немесе қате көрсетілуі үшін, қате кодын файлға сақтайтын орындалатын .bat файлын жасаңыз, мысалы:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Содан кейін жаңадан жасалған орнату пакеті қалтасында Kaspersky Security Center жасаған .kud файлдарын өзгертіңіз:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

Бұл жағдайда, атап көрсетілгендерден ерекшеленетін кез келген код қатені білдіреді.

Тапсырманың нәтижелерінде тапсырманың сәтті аяқталғаны туралы түсініктемесі жазылған жол немесе қателер туралы хабар көрсетілуі үшін, [SetupProcessResult_SuccessCodes] және [SetupProcessResult_ErrorCodes] секцияларында процесті қайтару кодтарына сай келетін қателердің қысқаша сипаттамаларын белгілеу керек, мысалы:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

Kaspersky Security Center бағдарламасының құрылғыны қайта іске қосуды басқару бойынша құралдарын қолдану үшін (қайта іске қосу операцияны аяқтау үшін керек болса), онда [SetupProcessResult_NeedReboot] секциясында қайта іске қосу қажеттілігін білдіретін процесті қайтару кодтарын қосымша түрде атап көрсету керек:

```
[SetupProcessResult_NeedReboot]
3010=
```

Орналастыру мониторингі

Kaspersky Security Center орналастыруды бақылау, сондай-ақ басқарылатын құрылғыларда қауіпсіздік бағдарламасы мен Желілік агенттің болуын бақылау үшін **Орналастыру** блогындағы түрлі-түсті индикаторға назар аудару керек. Индикатор Басқару консолінің негізгі терезесіндегі Басқару сервері түйінің жұмыс аймағында орналасқан. Индикатор орналастырудың ағымдағы күйін көрсетеді. Индикатордың жанында Желілік агенттері мен қауіпсіздік бағдарламалары орнатылған құрылғылар саны көрсетіледі. Белсенді орнату тапсырмалары болған кезде, тапсырмаларды орнату прогресі көрсетіледі. Орнату қателері болған кезде, мұнда қателердің саны көрсетіледі. Қате туралы егжей-тегжейлі ақпаратты сілтеме арқылы қарап шығуға болады.

Сонымен қатар, **Топтар** қойыншасында **Басқарылатын құрылғылар** қалтасының жұмыс аймағын орналастыру диаграммасын пайдалануға болады. Диаграмма орналастыру процесін көрсетеді: Желілік агенті жоқ, Желілік агенті бар, Желілік агенті пен қауіпсіздік бағдарламасы бар құрылғылардың саны.

Орналастыру барысының (немесе нақты орнату тапсырмасының) барынша егжей-тегжейлі сипаттамасын тиісті қашықтан орнату тапсырмасын орындау нәтижелері терезесінде көруге болады: Тапсырманың мәнмәтіндік мәзірінен **Нәтижелер** тармағын таңдаңыз. Терезеде екі тізім көрсетіледі: жоғарғы тізімде құрылғылардағы тапсырма күйлерінің тізімі, ал төменгі тізімде – қазіргі уақытта жоғарғы тізімде таңдалған құрылғыдағы тапсырма оқиғаларының тізімі бар.

Орналастыру кезіндегі қателер туралы ақпарат Басқару серверінің Kaspersky Event журналына жазылады. Қате туралы ақпарат **Оқиғалар** қойыншасындағы Басқару сервері түйініндегі тиісті оқиғалар таңдауында да қолжетімді.

Инсталляторлар параметрлерін конфигурациялау

Бөлім Kaspersky Security Center инсталляторлар файлдары және орнату параметрлері туралы ақпаратты, сондай-ақ басқару серверін және желілік агентті "тыныш" режимде орнату жөніндегі ұсынымдарды қамтиды.

Жалпы ақпарат

Kaspersky Security Center 15.1 құрамдастары – Басқару сервері, Желілік агент, Басқару консолінің инсталляторлары Windows Installer технологиясына негізделген. Инсталлятордың өзегі – MSI пакеті болып саналады. Дистрибутив қаптамасының осындай пішімі Windows Installer технологиясының барлық артықшылықтарын қолдануға мүмкіндік береді: масштабталу, патчтау жүйесін, түрлендіру жүйесін қолдану мүмкіндігі, үшінші тарап шешімдерімен орталықтандырылған түрде орнату мүмкіндігі, операциялық жүйеде тіркелу айқындығы.

Тыныш режимде орнату (жауаптар файлымен)

Басқару сервері мен Желілік агенттің инсталляторларында, пайдаланушының қатысуынсыз тыныш режимде орнатуға арналған параметрлер жазылған жауаптар файлымен (ss_install.xml) жұмыс істеу мүмкіндігі іске асырылған. ss_install.xml файлы MSI пакетімен бір қалтада орналасқан және тыныш режимде орнату кезінде автоматты түрде қолданылады. Сіз "/s" пәрмен жолының кілті арқылы автоматты түрде орнату режимін қоса аласыз.

Іске қосу мысалы:

```
setup.exe /s
```

Орнатушы бағдарламасын тыныш режимде іске қоспас бұрын, Лицензиялық келісімді оқып шығыңыз. Kaspersky Security Center дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады.

ss_install.xml файлы Kaspersky Security Center инсталляторы параметрлерінің ішкі пішімі болып табылады. Дистрибутивтер құрамында әдепкі бойынша параметрлері бар ss_install.xml файлы жеткізіледі.

ss_install.xml файлын қолмен өзгертудің қажеті жоқ. Бұл файл, Басқару консолідегі орнату пакеттерінің параметрлерін өзгерту кезінде Kaspersky Security Center құралдарымен өзгертіледі.

Басқару серверін орнату үшін жауап файлын өзгерту үшін:

1. Kaspersky Security Center дистрибутивін ашыңыз. EXE файлының толық пакетін қолдансаңыз, оны мұрағаттан шығарыңыз.

2. Сервер қалтасын қалыптастырыңыз, пәрмен жолын ашыңыз және келесі пәрменді орындаңыз:

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center орнату бағдарламасы іске қосылады.

3. Kaspersky Security Center орнатуды конфигурациялау үшін шебердің нұсқауларын орындаңыз.

Шебердің жұмысы аяқталғаннан кейін, жауаптар файлы сіз көрсеткен жаңа параметрлерге сай автоматты түрде өзгертіледі.

Желілік агентті тыныш режимде орнату (жауаптар файлы жоқ)

Желілік агент, MSI сипаттарының мәндерін стандартты түрде белгілей отырып, тек бір msi пакетінің көмегімен орнатылуы мүмкін. Мұндай сценарий топтық саясатты қолдана отырып, Желілік агентті орнатуға мүмкіндік береді.

Kaspersky Network Agent.msi орнату пакетінің атын өзгертпеңіз. Пакет атауы өзгертілсе, желілік агентті жаңартқан кезде орнату қателері пайда болуы мүмкін.

MSI сипаттары арқылы берілген параметрлер мен жауап файлында берілген параметрлер арасында қайшылық болмас үшін `DONT_USE_ANSWER_FILE=1` сипатын белгілеу арқылы жауап файлын өшіру мүмкіндігі қарастырылған. MSI файлы Kaspersky Security Center бағдарламасының дистрибутивінде Packages\NetAgent\exec қалтасында орналасқан. Төменде msi пакетін пайдаланып Желілік агент инсталляторын іске қосудың мысалы келтірілген.

Желілік агентті интерактивті емес режимде орнату Лицензиялық келісімді қабылдауды талап етеді. `EULA=1` параметрін тек Лицензиялық келісімнің шарттарын толық оқып, түсініп, қабылдаған жағдайда ғана қолданыңыз.

Мысалы:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Сондай-ақ, түрлендіру файлын (mst кеңейтімі бар файл) алдын ала дайындау арқылы msi пакетін орнату параметрлерін белгілеуге болады. Пәрмен келесідей болады:

Мысалы:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Бір пәрменде бірнеше түрлендіру файлын көрсетуге болады.

Windows Installer көмегімен желі агентін жаңартқыңыз келсе, келесі пәрменді орындаңыз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

setup.exe арқылы орнату параметрлерін ішінара конфигурациялау

setup.exe арқылы бағдарламаларды орнатуды іске қосу арқылы кез келген MSI сипаттарының мәндерін MSI пакетіне жіберуге болады.

Пәрмен келесідей болады:

Мысалы:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Басқару серверін орнату параметрлері

Төмендегі кестеде, Басқару серверін орнату кезінде конфигурациялауға болатын MSI сипаттары сипатталған. EULA және PRIVACYPOLICY қоспағанда, барлық параметрлер міндетті емес.

Басқару серверін тыныш режимде орнату параметрлері

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
EULA	Лицензиялық келісімнің шарттарымен келісу (міндетті параметр)	• 1 – Мен Лицензиялық келісімді толығымен оқып шыққанымды және оның шарттарын қабылдайтынымды растаймын. • Басқа мән немесе белгіленбеген – Лицензиялық келісімнің шарттарымен келіспейсіз (орнату жүзеге асырылмайды).
PRIVACYPOLICY	Құпиялық саясатының шарттарымен келісу (міндетті параметр)	• 1 – Менің деректерім Құпиялылық саясатында сипатталғандай өңделетінін және тасымалданатынын (соның ішінде үшінші тараптарға) білемін және оған келісемін. Құпиялылық саясатын толықтай оқып, түсінгенімді растаймын. • Басқа мән немесе белгіленбеген – Мен Құпиялылық саясатының шарттарын қабылдамаймын (орнату орындалмайды).
INSTALLATIONMODETYPE	Басқару серверін орнату түрі	• Стандартты. • Таңдаулы.
INSTALLDIR	Бағдарламаны орнату қалтасы	Жол мәні.
ADDLOCAL	Орнату үшін құрамдастар тізімі (үтір арқылы)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Басқару серверін дұрыс орнату үшін жеткілікті құрамдастардың минималды тізімі: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Желінің өлшемі	• NRT_1_100 – 1-ден 100 құрылғыға дейін. • NRT_100_1000 – 101-ден 1000 құрылғыға дейін. • NRT_GREATER_1000 – 1000-нан астам құрылғы.
SRV_ACCOUNT_TYPE	Басқару сервері қызметінің жұмыс істеуі үшін пайдаланушыны белгілеу тәсілі	• SrvAccountDefault – пайдаланушы есептік жазбасы автоматты түрде жасалады. • SrvAccountUser – пайдаланушы есептік жазбасы қолмен белгіленген.
SERVERACCOUNTNAME	Қызметке арналған пайдаланушы атауы	Жол мәні.
SERVERACCOUNTPWD	Қызмет үшін пайдаланушы құпиясөзі	Жол мәні.
DBTYPE	Дерекқор түрі	• MySQL – MySQL немесе MariaDB дерекқоры қолданылады. • MSSQL – Microsoft SQL Server (SQL Express) дерекқоры қолданылады.
MYSQLSERVERNAME	MySQL немесе MariaDB серверінің толық атауы	Жол мәні.
MYSQLSERVERPORT	MySQL немесе MariaDB серверіне қосылуға арналған порт нөмірі	Сандық мән.
MYSQLDBNAME	MySQL немесе MariaDB сервері дерекқорының атауы	Жол мәні.
MYSQLACCOUNTNAME	MySQL немесе MariaDB серверінің дерекқорына қосуға арналған пайдаланушы атауы	Жол мәні.

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
MYSQLACCOUNTPWD	MySQL немесе MariaDB серверінің дерекқорына қосуға арналған пайдаланушы құпиясөзі	Жол мәні.
MSSQLCONNECTIONTYPE	MSSQL дерекқорын қолдану түрі	• InstallMSSEE – пакеттен орнату. • ChooseExisting – орнатылған серверді қолдану.
MSSQLSERVERNAME	SQL Server үлгісінің толық атауы	Жол мәні.
MSSQLDBNAME	SQL Server дерекқорының атауы	Жол мәні.
MSSQLAUTHTYPE	SQL Server серверіне қосылу кезіндегі түпнұсқалық растама тәсілі	• Windows. • SQLServer.
MSSQLACCOUNTNAME	SQL Server серверіне SQLServer режимінде қосылу үшін пайдаланушы атауы	Жол мәні.
MSSQLACCOUNTPWD	SQL Server серверіне SQLServer режимінде қосылу үшін пайдаланушы құпиясөзі	Жол мәні.
CREATE_SHARE_TYPE	Ортақ қатынасы бар қалтаны белгілеу тәсілі	• Create – ортақ қатынасы бар жаңа қалтаны жасау. Бұл жағдайда, келесі сипаттар белгіленуі тиіс: • SHARELOCALPATH – жергілікті қалтаға апаратын жол. • SHAREFOLDERNAME – қалтаның желілік атауы. • Бос – EXISTSHAREFOLDERNAME сипаты белгіленуі тиіс.
EXISTSHAREFOLDERNAME	Қолданыстағы ортақ қатынасы бар қалтаға апаратын толық жол	Жол мәні.
SERVERPORT	Басқару серверіне қосылуға арналған порт нөмірі	Сандық мән.
SERVERSSLPORT	Басқару серверімен SSL қосылымын орнатуға арналған порт нөмірі	Сандық мән.
SERVERADDRESS	Басқару сервері мекенжайы	Жол мәні.
SERVERCERT2048BITS	Басқару серверінің сертификатына арналған кілттің ұзындығы (бит түрінде)	• 1 – Басқару серверінің сертификатына арналған кілттің ұзындығы 2048 битті құрайды. • 0 – Басқару серверінің сертификатына арналған кілттің ұзындығы 1024 битті құрайды. • Егер параметр белгіленбесе, онда Басқару серверінің сертификатына арналған кілттің ұзындығы 2048 битті құрайды.
MOBILESERVERADDRESS	Ұялы құрылғылар қосылатын Басқару серверінің мекенжайы; MobileSupport құрамдасы таңдалмаса, еленбейді	Жол мәні.

Желілік агентті орнату параметрлері

Төмендегі кестеде, Желілік агентті орнату кезінде конфигурациялауға болатын MSI сипаттары сипатталған. EULA және SERVERADDRESS қоспағанда, барлық параметрлер міндетті емес.

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
EULA	Лицензиялық келісімнің шарттарымен келісу	• 1 – мен осы Түпкі пайдаланушының лицензиялық келісімінің шарттары мен талаптарын толықтай оқып шығып, түсінгенімді растаймын және қабылдаймын. • 0 – Лицензиялық келісімнің шарттарын қабылдамаймын (орнату орындалмайды). • Мән белгіленбеген – Лицензиялық келісімнің шарттарын қабылдамаймын (орнату орындалмайды).
DONT_USE_ANSWER_FILE	Жауап файлынан орнату параметрлерін оқу.	• 1 – Қолданбау. • басқа мән немесе белгіленбеген – оқу.
INSTALLDIR	Желілік агентті орнату қалтасына апаратын жол.	Жол мәні.
SERVERADDRESS	Басқару серверінің мекенжайы (міндетті параметр).	Жол мәні.
SERVERPORT	Басқару серверіне қосылу портының нөмірі.	Сандық мән.
SERVERSSLPORT	SSL протоколын пайдаланып Басқару серверіне қауіпсіз қосылуға арналған порт нөмірі.	Сандық мән.
USESSL	SSL байланысын пайдалану керек пе.	• 1 – пайдалану; • басқа мән немесе белгіленбеген – пайдаланбау.
OPENUDPPORT	UDP портын ашу керек пе.	• 1 – ашу; • басқа мән немесе белгіленбеген – ашпау.
UDPPORT	UDP портының нөмірі.	Сандық мән.
USEPROXY	Прокси-серверді пайдалану керек пе. Үйлесімділік себептері бойынша Желілік агент орнату пакетінің параметрлерінде прокси-серверге қосылу параметрлерін көрсету ұсынылмайды.	• 1 – пайдалану; • басқа мән немесе белгіленбеген – пайдаланбау.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Прокси-сервер мекенжайы және прокси-серверге қосылуға арналған порт нөмірі.	Жол мәні.
PROXYLOGIN	Прокси-серверге қосылуға арналған есептік жазба.	Жол мәні.
PROXYPASSWORD	Прокси-серверге қосылуға арналған есептік жазбаның құпиясөзі (орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетіңіз).	Жол мәні.
GATEWAYMODE	Қосылым шлюзін пайдалану режимі.	• 0 – қосылымдар шлюзін пайдаланбау; • 1 – бұл Желілік агентті қосылым шлюзі ретінде пайдалану; • 2 – Басқару серверіне қосылым шлюзі арқылы қосылу.
GATEWAYADDRESS	Қосылым шлюзі мекенжайы.	Жол мәні.
CERTSELECTION	Сертификат алу тәсілі.	• GetOnFirstConnection – Басқару серверінен сертификат алу; • GetExistent — бар сертификатты таңдау. Бұл опция таңдалса, CERTFILE сипаты көрсетілуі керек.

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
CERTFILE	Сертификат файлының жолы.	Жол мәні.
VMVDI	VDI үшін динамикалық режимді қосу керек пе.	• 1 – қосу; • 0 – қоспау; • Мән белгіленбеген – қоспау.
VMOPTIMIZE	Желілік агенттің параметрлері гипервизор үшін оңтайлы ма.	• 1 – қосу; • 0 – қоспау; • Мән белгіленбеген – қоспау.
LAUNCHPROGRAM	Желілік агент қызметін орнатқаннан кейін іске қосу керек пе. VMVDI=1 болса, параметр еленбейді.	• 1 – іске қосу; • басқа мән немесе белгіленбеген – іске қоспау.
NAGENTTAGS	Желілік агентке арналған тег (жауап файлында көрсетілген тегтен басым).	Жол мәні.

Виртуалды инфрақұрылым

Kaspersky Security Center бағдарламасы виртуалды машиналармен жұмыс істеуді қолдайды. Сіз әр виртуалды машинада Желілік агент пен қауіпсіздік бағдарламаларын орната аласыз, сонымен қатар виртуалды машиналарды гипервизор деңгейінде қорғай аласыз. Бірінші жағдайда, виртуалды машиналарды қорғау үшін қарапайым қауіпсіздік бағдарламасын да, Kaspersky Security for Virtualization Light Agent бағдарламасын да қолдануға болады. Екінші жағдайда, Kaspersky Security for Virtualization Agentless бағдарламасын қолдана аласыз.

Kaspersky Security Center бағдарламасы виртуалды машиналарды алдыңғы күйге шегіндіру мүмкіндігін қолдайды.

Виртуалды машиналарға түсетін жүктемені азайту бойынша ұсынымдар

Желілік агентті виртуалды машинаға орнатқан жағдайда, виртуалды машиналар үшін өте пайдалы емес Kaspersky Security Center функционалдығының бір бөлігін өшіру туралы ойлану керек.

Желілік агентті виртуалды машинаға немесе болашақта виртуалды машиналар алынатын үлгіге орнатқан кезде келесі әрекеттерді орындау ұсынылады:

- қашықтан орнату орындалып жатса, Желілік агенттің орнату пакетінің сипаттар терезесінде (**Кеңейтілген** бөлімінде) **VDI параметрлерін оңтайландыру** параметрін таңдаңыз;
- егер шебердің көмегімен интерактивті орнату орындалып жатса, шебер терезесінде **Виртуалды инфрақұрылым үшін Желілік агент параметрлерін оңтайландыру** параметрін таңдаңыз.

Параметрлерді таңдау, Желілік агенттің параметрлерін, әдепкі бойынша (саясатты қолданар алдында) келесі функциялар өшірілетіндей етіп өзгертеді:

- Орнатылған бағдарламалық жасақтама туралы ақпарат алу
- Аппараттық жасақтама туралы ақпарат алу
- Осалдықтардың болуы туралы ақпарат алу
- Қажетті жаңартулар туралы ақпарат алу

Әдетте, аталған функциялар виртуалды машиналарда қажет емес, өйткені олардағы бағдарламалық жасақтама мен виртуалды аппараттық жасақтама біркелкі.

Функцияларды өшіру қайтымды. Егер өшірулі функциялардың кез келгені қажет болса, оны Желілік агент саясаты немесе Желілік агенттің жергілікті параметрлері арқылы қосуға болады. Желілік агенттің жергілікті параметрлері Басқару консоліндегі тиісті құрылғының контекстік мәзірінен қолжетімді.

Динамикалық виртуалды машиналарды қолдау

Kaspersky Security Center динамикалық виртуалды машиналарды қолдайды. Егер ұйымның желісінде виртуалды инфрақұрылым орналастырылған болса, онда кейбір жағдайларда динамикалық (уақытша) виртуалды машиналар қолданылуы мүмкін. Мұндай машиналар, әкімші алдын ала дайындаған үлгіден ерекше атаулармен жасалады. Пайдаланушы жасалған машинамен біраз уақыт жұмыс істейді, ал виртуалды машина өшірілгеннен кейін виртуалды инфрақұрылымнан жойылады. Егер ұйымның желісінде Kaspersky Security Center орналастырылған болса, оған орнатылған Желілік агенті бар виртуалды машина Басқару серверінің дерекқорына қосылады. Виртуалды машинаны өшіргеннен кейін, ол туралы жазба Басқару сервері дерекқорынан да жойылуы керек.

Виртуалды машина жазбаларын автоматты түрде жою функционалдығы жұмыс істеуі үшін Желілік агентті динамикалық виртуалды машиналар жасалатын үлгіе орнатқан кезде **VDI үшін динамикалық режимді қосу** параметрін таңдау керек:

- қашықтан орнату жағдайында – Желілік агенттің орнату пакетінің сипаттары терезесінде (**Кеңейтілген** бөлімі);
- интерактивті орнату жағдайында – Желілік агентті орнату шеберінде.

VDI үшін динамикалық режимді қосу параметрі Желілік агентті физикалық құрылғыларға орнатқан кезде таңдалмауы керек.

Машиналар жойылғаннан кейін Динамикалық виртуалды машиналардағы оқиғалар біраз уақыт бойы Басқару серверінде сақталуы керек болса, онда Басқару сервері сипаттары терезесінде, **Оқиғалар қоймасы** бөлімінде **Құрылғылар жойылғаннан кейін оқиғаларды сақтау** параметрін таңдап, күндердегі оқиғаларды сақтаудың ең ұзақ уақытын көрсету керек.

Динамикалық виртуалды машиналарда дискіні шифрлауды қосуға кеңес бермейміз.

Виртуалды машиналарды көшіруді қолдау

Виртуалды машинаны орнатылған Желілік агентімен бірге көшіру немесе оны орнатылған Желілік агентпен бірге үлгіден жасау – қатты дискінің кескінін түсіру және көшіру арқылы Желілік агенттерді орналастыруға тең келеді. Сондықтан, жалпы жағдайда, виртуалды машиналарды көшіру кезінде диск кескінін көшіру арқылы орналастыру сияқты әрекеттерді орындау қажет.

Алайда, төменде сипатталған екі жағдайда Желілік агент көшіру фактісін автоматты түрде анықтайды. Сондықтан, "Құрылғының қатты дискісін түсіру және көшіру" бөлімінде сипатталған күрделі әрекеттерді орындау міндетті емес:

- Желілік агентті орнату кезінде **VDI үшін динамикалық режимді қосу** параметрі таңдалды: операциялық жүйені әрбір рет қайта іске қосқаннан кейін мұндай виртуалды машина, оны көшіру фактісіне қарамастан, жаңа құрылғы болып саналатын болады.

- Келесі гипервизорлардың бірі қолданылады: VMware™, HyperV® немесе Xen®: Желілік агент виртуалды машинаны көшіру фактісін виртуалды аппараттық жасақтаманың өзгерген идентификаторлар бойынша анықтайды.

Виртуалды аппараттық жасақтаманың өзгерістерін талдау мүлдем сенімді емес. Бұл әдісті кеңінен қолданбас бұрын, оның жұмысқа жарамдылығын ұйымда қолданылатын гипервизордың нұсқасы үшін аздаған виртуалды машиналарда алдын ала тексеріп алу керек.

Желілік агенті бар құрылғылар үшін файлдық жүйені шегіндіруді қолдау

Kaspersky Security Center бағдарламасы таратылған бағдарлама болып саналады. Желілік агенті орнатылған құрылғылардың бірінде файлдық жүйені алдыңғы күйге шегіндіру деректерді синхрондамауға және Kaspersky Security Center дұрыс жұмыс істемеуіне әкеледі.

Файлдық жүйені (немесе оның бір бөлігін) алдыңғы күйге шегіндіру келесі жағдайларда болуы мүмкін:

- қатты дискінің кескінін көшіру кезінде;

- виртуалды инфрақұрылым арқылы виртуалды машинаның күйін қалпына келтіру кезінде;

- сақтық көшірмеден немесе қалпына келтіру нүктесінен деректерді қалпына келтіру кезінде.

Kaspersky Security Center үшін, Желілік агенті орнатылған құрылғылардағы үшінші тарап бағдарламалық жасақтамасы %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ қалтасына әсер ететін сценарийлер ғана маңызды. Сондықтан, мүмкіндік болса, бұл қалтаны қалпына келтіру процедурасынан әрқашан алып тастап отыру керек.

Бірқатар ұйымдарда жұмыс регламенті құрылғылардың файлдық жүйесінің күйін шегіндіруді көздейтіндіктен, Kaspersky Security Center бағдарламасында, 10 Maintenance Release 1 нұсқасынан бастап (Басқару сервері мен Желілік агенттер нұсқасы 10 Maintenance Release 1 немесе одан жоғары болуы керек), Желілік агенті орнатылған құрылғыларда файлдық жүйенің шегіндірілуін анықтауды қолдау мүмкіндігі қосылды. Табылған жағдайда, мұндай құрылғылар деректерді толық тазалаумен және толық синхрондаумен бірге Басқару серверіне автоматты түрде қайта қосылады.

Kaspersky Security Center 15.1 нұсқасында файлдық жүйенің шегіндірілуін анықтауды қолдау әдепкі бойынша қосылады.

Кез келген мүмкіндік туындаған кезде, %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ қалтасын Желілік агенті орнатылған құрылғыларға шегіндіруден аулақ болу керек, өйткені деректерді толық қайта синхрондау көп ресурстарды қажет етеді.

Басқару сервері орнатылған құрылғы үшін жүйенің күйін шегіндіруге жол берілмейді. Басқару сервері пайдаланатын дерекқордың алдыңғы күйіне шегіндіру де қолайсыз.

Сақтық көшірмеден Басқару серверінің күйін тек штаттық klbackup утилитасын пайдаланып қалпына келтіруге болады.

Бағдарламаларды жергілікті түрде орнату

Бұл бөлімде құрылғыларға тек жергілікті жерде орнатуға болатын бағдарламаларды орнату процедурасы сипатталған.

Таңдалған клиент құрылғысында бағдарламаларды жергілікті түрде орнатуды жүзеге асыру үшін сіз осы құрылғыда әкімші құқығына ие болуыңыз керек.

Бағдарламаларды таңдалған клиент құрылғысына жергілікті түрде орнату үшін:

1. Клиент құрылғысына Желілік агент орнатыңыз және клиент құрылғысы мен Басқару сервері арасында байланыс орнатыңыз.

2. Осы бағдарламаларға арналған Нұсқаулықтарда көрсетілген сипаттамаларға сәйкес құрылғыға қажетті бағдарламаларды орнатыңыз.

3. Орнатылған бағдарламалардың әрқайсысы үшін басқару плагинін әкімшінің жұмыс орнына орнатыңыз.

Сонымен қатар, Kaspersky Security Center жеке орнату пакетін пайдаланып бағдарламаларды жергілікті түрде орнату мүмкіндігін қолдайды. Kaspersky Security Center бағдарламасы Kaspersky бағдарламаларының барлығын орнатуды қолдамайды.

Желілік агентті жергілікті орнату

Құрылғыға Желілік агентті жергілікті түрде орнату үшін:

1. Құрылғыда setup.exe файлын интернет арқылы алынған дистрибутивтен іске қосыңыз. Қосымша ақпарат алу үшін келесі бөлімдерді қараңыз: Kaspersky Security Center жеткізу жиынтығынан Желілік агентті орнату пакетін алу.

   Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады.

2. **Kaspersky Security Center Желілік агентін ғана орнатыңыз** сілтемесі бойынша бағдарламаларды таңдау терезесінде Желілік агентті орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

   a. **Басқару сервері**

      Порт

      Желілік агенттерден қосылымдарды қабылдау үшін Басқару сервері пайдаланатын қорғалмаған порт көрсетілген.

      Әдепкі бойынша порт нөмірі – 14000.

      SSL порты

      Желілік агенттерден қосылымдарды алу үшін Басқару сервері пайдаланатын SSL порты көрсетілген.

      Әдепкі бойынша порт нөмірі – 13000.

Басқару серверіне қосылу үшін SSL пайдалану

Бұл параметр қосулы болса, Басқару серверіне қосылу SSL протоколының көмегімен, қорғалған порт арқылы орындалатын болады.

Әдепкі бойынша, параметр қосулы.

Желілік агентке UDP портын ашуға рұқсат ету

Бұл параметр қосылса, орнату бағдарламасы клиент құрылғысын басқару және ол туралы ақпаратты алу үшін Басқару сервері пайдаланатын портты автоматты түрде ашады.

Әдепкі бойынша, параметр қосулы.

UDP порты

Клиент құрылғысын басқару және ол туралы ақпаратты алу үшін Басқару сервері пайдаланатын портты конфигурациялауға мүмкіндік береді.

Әдепкі бойынша порт нөмірі – 15000.

b. **Прокси-сервердің конфигурациясы**

Прокси-серверді пайдалану

Бұл параметр қосылса, прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

Әдепкі бойынша, параметр өшірулі.

Мекенжай

Порт

Есептік жазба

Прокси-серверге қосылым орындалатын есептік жазба пайдаланушысының атауы.

Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

Құпиясөз

Прокси-серверге қосылым орындалатын есептік жазба құпиясөзі.

Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

c. **Қосылым шлюзі**

Қосылым шлюзін пайдаланбау

Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану

Желілік агентті, деректер жіберу уақытында Басқару серверіне қосылу, онымен байланысу және деректерді Желілік агентте қауіпсіз жерде сақтау үшін демилитаризацияланған аймақтағы қосылым шлюзі (DMZ) ретінде қолдану үшін бұл параметрді таңдаңыз.

Басқару серверіне байланыс шлюзі арқылы қосылу

Осы параметрді таңдап, қосылым шлюзі ретінде әрекет ететін құрылғыны көрсетіңіз.

d. **Басқару серверінің сертификаты**

e. **Агенттің тегтері**

f. **Қосымша параметрлер**

Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату

Бұл параметрді қосулы күйде қалдыру ұсынылады. Kaspersky Security Center құрамдастарына арналған автоматты жаңартуларды және патчтарды орнатуды өшіру үшін бұл жалаушаны алып тастай аласыз. Әкімші автоматты орнатуды кейінірек саясаттың көмегімен қоса алады.

Әдепкі бойынша, параметр өшірулі.

Желілік агент қызметін қорғау функциясын қосу

Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, құрамдасты қажетті құқықтарсыз жою немесе өзгерту мүмкін емес. Желілік агенттің жұмысын тоқтату мүмкін емес. Бұл параметр домен контроллерлеріне әсер етпейді.

Жергілікті әкімші құқықтарымен басқарылатын жұмыс станцияларында Желілік агентті қорғау үшін осы параметрді қосыңыз.

Әдепкі бойынша, параметр өшірулі.

VDI үшін динамикалық режимді қосу

Параметр қосулы болса, виртуалды машинада орнатылған Желілік агент үшін Virtual Desktop Infrastructure (VDI) үшін динамикалық режим қосылады.

Әдепкі бойынша, параметр өшірулі.

VDI үшін Kaspersky Security Center желілік агент параметрлерін оңтайландырыңыз. Осалдықты сканерлеуді және қолданбалар мен аппараттық құралдарды түгендеуді өшіріңіз. Желілік агент саясатын қолдана отырып, белгіленген параметрлерді өзгерте аласыз.

Егер параметр қосулы болса, Желілік агенттің параметрлерінде келесі функциялар өшіріледі:

- Орнатылған бағдарламалық жасақтама туралы ақпарат алу
- Аппараттық жасақтама туралы ақпарат алу
- Осалдықтардың болуы туралы ақпарат алу
- Қажетті жаңартулар туралы ақпарат алу

Әдепкі бойынша, параметр өшірулі.

g. **Бағдарламаны іске қосу**

Орнату шеберінің жұмысы аяқталғаннан кейін, құрылғыға Желілік агент орнатылады.

Сіз Kaspersky Security Center Желілік агенті қызметінің сипаттарын көре аласыз, сонымен қатар Microsoft Windows стандартты құралдары: Компьютерді басқару\Қызметтер арқылы Желілік агенттің белсенділігін іске қоса, тоқтата және бақылай аласыз.

Желілік агентті тыныш режимде орнату

Желілік агентті тыныш режимде орнатуға болады, яғни орнату параметрлерін интерактивті түрде енгізбестен. Тыныш орнату үшін Желілік агенттің Windows Installer пакеті (MSI) қолданылады. MSI файлы Kaspersky Security Center бағдарламасының дистрибутивінде Packages\NetAgent\exec қалтасында орналасқан.

Kaspersky Network Agent.msi орнату пакетінің атын өзгертпеңіз. Пакет атауы өзгертілсе, желілік агентті жаңартқан кезде орнату қателері пайда болуы мүмкін.

MSI пакетінен желілік агентті тек тыныш режимде орнатуға болады, MSI пакетінен интерактивті орнатуға қолдау көрсетілмейді.

Жергілікті құрылғыда Желілік агентті тыныш режимде орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімді оқып шықсаңыз және оның шарттарын қабылдасаңыз, төмендегі пәрменді қолданыңыз.

2. Келесі пәрменді орындаңыз:

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   мұндағы `setup_parameters` – бір-бірінен бос орын арқылы бөлінген параметрлер мен олардың мәндерінің тізімі (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Параметрлер тізіміне `EULA=1` параметрін қосуыңыз керек. Әйтпесе, Желілік агент орнатылмайды.

Егер сіз қашықтағы құрылғыларда Kaspersky Security Center және Желілік агент үшін стандартты қосылым параметрлерін қолдансаңыз, келесі пәрменді орындаңыз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` – оқиғалар журналына жазу кілті. Оқиғалар журналы Желілік агентті орнатқан кезде жасалады және C:\windows\temp\nag_inst.log қалтасында сақталады.

nag_inst.log файлынан басқа, бағдарлама орнату оқиғаларының журналын қамтитын $klssinstlib.log файлын жасайды. Бұл файл %windir%\temp немесе %temp% қалтасында сақталады. Ақауларды жою үшін сізге немесе Kaspersky Техникалық қолдау қызметінің маманына екі журнал файлы қажет болуы мүмкін – nag_inst.log және $klssinstlib.log.

Басқару серверіне қосылу үшін портты қосымша көрсету қажет болса, келесі пәрменді енгізіңіз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

SERVERPORT параметрі Басқару серверіне қосылу портының нөміріне сәйкес келеді.

Желілік агентті тыныш режимде орнату кезінде қолдануға болатын параметрлердің аттары мен ықтимал мәндері Желілік агентті орнату параметрлері бөлімінде келтірілген.

Windows Installer көмегімен желі агентін жаңартқыңыз келсе, келесі пәрменді орындаңыз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Linux үшін Желілік агентті тыныш режимде орнату (жауап файлымен)

Сіз Linux операциялық жүйесі бар құрылғыларға Желілік агентті жауап файлы – орнату параметрлерінің пайдаланушы жиынтығын қамтитын мәтіндік файл: айнымалылар және олардың сәйкес мәндері арқылы орната аласыз. Жауаптар файлын қолдану арқасында орнатуды тыныш режимде, яғни пайдаланушының қатысуынсыз іске қосуға болады.

Linux үшін Желілік агентті тыныш режимде орнату мақсатында:

1. Linux операциялық жүйесі бар қажетті құрылғыны қашықтан орнату үшін дайындап қойыңыз. Кез келген лайықты пакеттерді басқару жүйесінің көмегімен .deb немесе .rpm Желілік агент пакетін қолдана отырып, қашықтан орнату пакетін жүктеңіз және жасаңыз.

2. SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

   Желілік агентті RED OS 7.3.4 не одан кейінгі нұсқадағы немесе MSVSPHERE 9.2 не одан кейінгі нұсқадағы операциялық жүйені қолданатын құрылғыларға орнатқыңыз келсе, желілік агенттің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

3. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімнің шарттарын түсініп, қабылдаған жағдайда ғана төмендегі қадамдарды орындаңыз.

4. Жауап файлын (TXT форматында) жасаңыз. Жауап файлына VARIABLE_NAME = variable_value пішіміндегі айнымалылар тізімін қосыңыз, әр айнымалы бөлек жолда тұрады.

   Жауап файлын дұрыс пайдалану үшін оған үш міндетті айнымалының ең аз жиынтығын қосу керек:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Қашықтан орнатудың барынша нақты параметрлерін пайдалану үшін кез келген қосымша айнымалыларды қосуға болады. Келесі кестеде жауап файлына енгізуге болатын барлық айнымалылар келтірілген:

   Тыныш режимде Linux үшін Желілік агентті орнату параметрлері ретінде пайдаланылатын жауап файлының айнымалылары

   Тыныш режимде Linux үшін Желілік агентті орнату параметрлері ретінде пайдаланылатын жауап файлының айнымалылары

Айнымалының атауы	Міндетті	Сипаттамасы	Ықтимал мәндер
KLNAGENT_SERVER	Иә	Толық домендік атау (FQDN) немесе IP мекенжайы ретінде ұсынылған Басқару сервері атауын қамтиды.	Құрылғының DNS атауы немесе IP мекенжайы.

KLNAGENT_AUTOINSTALL	Иә	Тыныш орнату режимі қосылғанын анықтайды.	1 – тыныш режим қосулы; орнату кезінде пайдаланушыға ешқандай әрекет ұсынылмайды. Басқасы – тыныш режим өшірулі; орнату кезінде пайдаланушыға әрекеттер ұсынылуы мүмкін.
EULA_ACCEPTED	Иә	Пайдаланушы Желілік агенттің Лицензиялық келісімін қабылдап-қабылдамайтынын анықтайды; егер айнымалы көрсетілмесе, оны Лицензиялық келісімді қабылдамау деп түсіндіруге болады.	1 – Мен осы Түпкі пайдаланушының лицензиялық келісімінің ережелері мен шарттарын толық оқып шықтым, түсіндім және қабылдаймын. Басқа мән немесе белгіленбеген – Лицензиялық келісімнің шарттарымен келіспеймін (орнату жүзеге асырылмайды).
KLNAGENT_PROXY_USE	Жоқ	Басқару серверімен орнатылған қосылым прокси-сервердің параметрлерін қолданады ма екенін анықтайды. Әдепкі бойынша, 0 мәні көрсетілген.	1 – прокси-сервер параметрлері қолданылады. Басқасы – прокси-сервер параметрлері қолданылмайды.
KLNAGENT_PROXY_ADDR	Жоқ	Басқару серверімен байланыс орнату үшін қолданылатын прокси-сервер мекенжайын анықтайды.	Құрылғының DNS атауы немесе IP мекенжайы.
KLNAGENT_PROXY_LOGIN	Жоқ	Прокси-серверге кіру үшін қолданылатын пайдаланушы атын анықтайды.	Кез келген қолданыстағы пайдаланушы аты.
KLNAGENT_PROXY_PASSWORD	Жоқ	Прокси-серверге кіру үшін қолданылатын пайдаланушы құпиясөзін анықтайды.	Операциялық жүйедегі әріптер мен сандардың, пішіммен рұқсат етілген құпиясөздің кез келген жиынтығы.
KLNAGENT_VM_VDI	Жоқ	Динамикалық виртуалды машиналарды жасау үшін кескінге Желілік агенттің орнатылып-орнатылмағанын анықтайды.	1 – Желілік агент динамикалық виртуалды машиналарды жасау үшін қолданылатын кескінге орнатылған. Басқасы – орнату барысында кескін қолданылмайды.
KLNAGENT_VM_OPTIMIZE	Жоқ	Желілік агенттің параметрлері гипервизор үшін оңтайлы ма екенін анықтайды.	1 – Желілік агенттің әдепкі бойынша жергілікті параметрлері, гипервизорда қолдануды оңтайландыра алатындай етіп өзгертілген.
KLNAGENT_TAGS	Жоқ	Желілік агенттің үлгісіне тағайындалған тегтерді атап көрсетеді.	Нүктелі үтірмен бөлінген бір немесе бірнеше тег.
KLNAGENT_UDP_PORT	Жоқ	Желілік агент қолданатын UDP портын анықтайды. Әдепкі бойынша, 15000 мәні көрсетілген.	Кез келген қолданыстағы порт нөмірі.
KLNAGENT_PORT	Жоқ	Желілік агент қолданбайтын портты (TLS емес) анықтайды. Әдепкі бойынша, 14000 мәні көрсетілген.	Кез келген қолданыстағы порт нөмірі.
KLNAGENT_SSLPORT	Жоқ	Желілік агент қолданатын TLS портын анықтайды. Әдепкі бойынша, 13000 мәні көрсетілген.	Кез келген қолданыстағы порт нөмірі.
KLNAGENT_USESSL	Жоқ	Қосылу үшін тасымал деңгейінің (TLS) қауіпсіздігі қолданылады ма екенін анықтайды.	1 (әдепкі бойынша) – TLS қолданылады. Басқасы – TLS қолданылмайды.

KLNAGENT_GW_MODE	Жоқ	Қосылым шлюзі пайдаланылады ма екенін анықтайды.	1 (әдепкі бойынша) – ағымдағы параметрлер өзгертілмейді (бірінші қоңырау кезінде қосылым шлюзі көрсетілмейді). 2 – қосылым шлюзі қолданылмайды. 3 – қосылым шлюзі қолданылады. KLNAGENT_GW_ADDRESS қажет. 4 – Желілік агент үлгісі демилитаризацияланған аймақта (DMZ) қосылым шлюзі ретінде пайдаланылады. Сервер сертификаты қажет.
KLNAGENT_GW_ADDRESS	Жоқ	Қосылым шлюзінің мекенжайын анықтайды. Мән, KLNAGENT_GW_MODE = 3 болса ғана қолданылады.	Құрылғының DNS атауы немесе IP мекенжайы.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Жоқ	Желілік агентті орнатқаннан кейін пайдаланушыны құрылғы иесі ретінде тіркеу үшін утилитаны іске қосуға мүмкіндік береді. Өшірілген болса, пайдаланушыға құрылғы иесі ретінде тіркелу қолжетімді емес.	1 — пайдаланушыны құрылғы иесінің утилитасы ретінде тіркеу желілік агентті орнатқаннан кейін іске қосылады. Басқа жағдайда — өшірілген.

5. Желілік агентті орнату пакетін іске қосыңыз. Жауап файлының жолын көрсететін KLAUTOANSWERS ортасының айнымалысы орнату пәрменіне жіберіледі. Келесі пәрмендердің бірін орындаңыз:

   - Желілік агентті RPM пакетінен 32 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> yum install ./klnagent-<құрастыру нөмірі>.i386.rpm`

   - Желілік агентті RPM пакетінен 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> yum install ./klnagent64-<құрастыру нөмірі>.x86_64.rpm`

   - Желілік агентті RPM пакетінен Arm архитектурасына арналған 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> yum install ./klnagent64-<құрастыру нөмірі>.aarch64.rpm`

   - Желілік агентті DEB пакетінен 32 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> apt install ./klnagent_<құрастыру нөмірі>_i386.deb`

   - Желілік агентті DEB пакетінен 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> apt install ./klnagent64_<құрастыру нөмірі>_amd64.deb`

   - Желілік агентті DEB пакетінен Arm архитектурасына арналған 64 биттік операциялық жүйеге орнату үшін келесі пәрменді орындаңыз:
     `sudo KLAUTOANSWERS=<жауап файлының жолы> apt install ./klnagent64_<құрастыру нөмірі>_arm64.deb`

   Операциялық жүйе конфигурациясына байланысты желілік агентті орнату үшін rpm, dpkg немесе dnf пакет менеджерлерін де пайдалануға болады.

Linux үшін Желілік агентті орнату тыныш режимде басталады; пайдаланушыдан процесс кезінде ешқандай әрекеттерді орындау сұралмайды.

Желілік агентті орнату үшін жабық бағдарлама ортасы режимінде Astra Linux басқаратын құрылғыны дайындау

Жабық бағдарлама ортасы режимінде Astra Linux жұмыс істейтін құрылғыға желілік агентті орнатпас бұрын екі дайындық процедурасын орындау керек: біреуі төмендегі нұсқауларда сипатталған және Linux операциялық жүйесі жұмыс істейтін кез келген құрылғы үшін жалпы дайындық қадамдары.

Осы нұсқаулықтары пәрмендерді root есептік жазбасы астында іске қосыңыз.

Желілік агентті орнату үшін жабық бағдарлама ортасы режимінде Astra Linux жұмыс істейтін құрылғыны дайындау үшін:

1. `/etc/digsig/digsig_initramfs.conf` файлын ашыңыз және келесі параметрлерді көрсетіңіз:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Пәрмен жолында үйлесімділік пакетін орнату үшін келесі пәрменді енгізіңіз:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Бағдарлама кілті үшін директория жасаңыз:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg қолданба кілтін алдыңғы қадамда жасалған каталогке қойыңыз:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Kaspersky Security Center жөнелтім жинағында kaspersky_astra_pub_key.gpg кілті болмаса, бұл кілтті https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg сілтемесі арқылы жүктеп алуға болады.

5. Дискілердің жедел жадын жаңартыңыз:

   ```
   update-initramfs -u -k all
   ```

   Жүйені қайта жүктеңіз.

Linux құрылғысы желілік агентті орнатуға дайын. Желілік агентті қашықтан, интерактивті режимде немесе дыбыссыз режимде орнатуға болады.

Linux үшін Желілік агентті интерактивті режимде орнату

Бұл мақалада орнату параметрлерін кезең-кезеңімен көрсете отырып, Linux операциялық жүйесімен жұмыс істейтін құрылғыларға Желілік агентті интерактивті режимде орнату жолы сипатталады. Сондай-ақ, жауап файлын – орнату параметрлерінің пайдаланушы белгілеген баптауларын қамтитын мәтіндік файлды пайдалануға болады: айнымалылар және олардың сәйкес мәндері. Жауаптар файлын қолдану арқасында орнатуды тыныш режимде, яғни пайдаланушының қатысуынсыз іске қосуға болады.

> Желілік агентті RED OS 7.3.4 не одан кейінгі нұсқадағы немесе MSVSPHERE 9.2 не одан кейінгі нұсқадағы операциялық жүйені қолданатын құрылғыларға орнатқыңыз келсе, желілік агенттің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

Желілік агентті интерактивті режимде орнату үшін:

1. Желілік агентті орнату пакетін іске қосыңыз. Linux дистрибутивіңізге байланысты келесі пәрмендердің бірін орындаңыз:

   - 32 разрядты операциялық жүйесі бар құрылғыға RPM бумасынан Желілік агентті орнату үшін:

     ```
     # yum -i klnagent-<құрастыру нөмірі>.i386.rpm
     ```

   - 64 разрядты операциялық жүйесі бар құрылғыға RPM бумасынан Желілік агентті орнату үшін:

     ```
     # yum -i klnagent64-<құрастыру нөмірі>.x86_64.rpm
     ```

   - Arm архитектурасына арналған 64 разрядты операциялық жүйесі бар құрылғыға RPM бумасынан Желілік агентті орнату үшін:

     ```
     # yum -i klnagent64-<құрастыру нөмірі>.aarch64.rpm
     ```

   - 32 разрядты операциялық жүйесі бар құрылғыға DEB бумасынан Желілік агентті орнату үшін:

     ```
     # apt install ./klnagent_<құрастыру нөмірі>_i386.deb
     ```

   - 64 разрядты операциялық жүйесі бар құрылғыға DEB бумасынан Желілік агентті орнату үшін:

     ```
     # apt install ./klnagent64_<құрастыру нөмірі>_amd64.deb
     ```

   - Arm архитектурасына арналған 64 разрядты операциялық жүйесі бар құрылғыға DEB бумасынан Желілік агентті орнату үшін:

     ```
     # apt install ./klnagent64_<құрастыру нөмірі>_arm64.deb
     ```

2. Желілік агентті конфигурациялауды іске қосыңыз:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Лицензиялық келісімді оқып шығыңыз. Мәтін пәрмен жолы терезесінде көрсетіледі. Мәтіннің келесі бөлігін көру үшін бос орын пернесін басыңыз. Сұрау көрсетілген кезде келесі мәндердің бірін енгізіңіз:

   - Лицензиялық келісімнің шарттарын түсініп, қабылдасаңыз, `y` енгізіңіз.

   - Лицензиялық келісімнің шарттарын қабылдамасаңыз, `n` енгізіңіз. Желілік агентті қолдану үшін Лицензиялық келісімнің шарттарын қабылдауыңыз қажет.

   - Лицензиялық келісімді қайта көрсету үшін `r` теріңіз.

4. Басқару серверінің DNS атын немесе IP мекенжайын енгізіңіз.

5. Басқару сервері портының нөмірі енгізіңіз. Әдепкі бойынша порт нөмірі – 14000.

6. Басқару сервері SSL портының нөмірін енгізіңіз. Әдепкі бойынша порт нөмірі – 13000.

7. Желілік агент және Басқару сервері арасындағы трафик үшін SSL шифрлауын пайдаланғыңыз келсе, `y` енгізіңіз. Болмаса, `n` енгізіңіз.

8. Желілік агентті конфигурациялаудың келесі тәсілдерінің бірін таңдаңыз:

   - `[1]` – қосылым шлюзін конфигурацияламаңыз.

     Құрылғыңыз қосылу шлюзі ретінде әрекет етпейді және қосылу шлюзі арқылы Басқару серверіне қосылмайды.

   - `[2]` – қосылу шлюзін пайдаланбау.

     Құрылғыңыз Басқару серверіне қосылу шлюзі арқылы қосылмайды.

   - `[3]` – қосылу шлюзі арқылы Серверге қосылыңыз.

     Құрылғыңыз Басқару серверіне қосылу шлюзі арқылы қосылады.

   - `[4]` – қосылу шлюзі ретінде пайдалану.

     Құрылғыңыз қосылу шлюзі ретінде әрекет етеді.

Желілік агент Linux операциялық жүйесімен жұмыс істейтін құрылғыда орнатылған.

Бағдарламаны басқару плагинін жергілікті түрде орнату

Бағдарламаны басқару плагинін орнату үшін,

Басқару консолі орнатылған құрылғыда, осы бағдарламаның дистрибутивіне кіретін klcfginst.exe орындалатын файлын іске қосыңыз.

klcfginst.exe файлы Kaspersky Security Center басқара алатын барлық бағдарламалардың құрамына кіреді. Орнату, шебер тарапынан сүйемелденеді және параметрлерді конфигурациялауды қажет етпейді.

Бағдарламаларды тыныш режимде орнату

Бағдарламаны тыныш режимде орнату үшін:

1. Kaspersky Security Center бағдарламасының басты терезесін ашыңыз.

2. Консоль ағашының **Қашықтан орнату** қалтасында, **Орнату пакеттері** салынған қалтасында қажетті бағдарламаның орнату пакетін таңдаңыз немесе бұл бағдарлама үшін жаңа орнату пакетін жасаңыз.

   Орнату пакеті Басқару серверінде Packages қызметтік қалтасындағы ортақ қатынасы бар қалтада сақталады. Бұл жағдайда, әрбір орнату пакетіне жеке салынған қалта сәйкес келеді.

3. Қажетті орнату пакетінің қалтасын келесі тәсілдердің бірімен ашыңыз:

   - Қажетті орнату пакетіне сәйкес қалтаны Басқару серверінен клиент құрылғысына көшіріңіз. Содан кейін, клиент құрылғысында көшірілген қалтаны ашыңыз.

   - Клиент құрылғысынан Басқару серверінде қажетті орнату пакетіне сәйкес келетін ортақ қатынасы бар қалтаны ашыңыз.

   Егер ортақ қатынасы бар қалта Microsoft Windows Vista операциялық жүйесі орнатылған құрылғыларда орналасқан болса, **Пайдаланушылардың есептік жазбаларын басқару: барлық әкімшілер әкімшінің мақұлдауы режимінде жұмыс істейді** параметрі үшін **Өшірулі** мәнін белгілеу керек (**Бастау** → **Басқару тақтасы** → **Басқару** → **Жергілікті қауіпсіздік саясаты** → **Қауіпсіздік параметрлері**).

4. Таңдалған бағдарламаға байланысты келесі әрекеттерді орындаңыз:

   - Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers және Kaspersky Security Center үшін салынған exec қалтасына өтіп, /s кілті бар орындалатын файлды (exe кеңейтімі бар файлды) іске қосыңыз.

   - Kaspersky қалған бағдарламалары үшін /s кілті бар орындалатын файлды (exe кеңейтімі бар файлды) ашық қалтадан іске қосыңыз.

   `EULA=1` және `PRIVACYPOLICY=1` кілттері бар орындалатын файлды іске қосу, сіз сәйкесінше Лицензиялық келісім мен Құпиялық саясатын толығымен оқып шыққаныңызды, түсінгеніңізді және олардың ережелерін қабылдайтыныңызды білдіреді. Сондай-ақ, сіздің деректеріңіз Құпиялылық саясатында сипатталғандай өңделетінін және жіберілетінін (соның ішінде үшінші елдерге) білесіз. Лицензиялық келісімнің мәтіні және Құпиялылық саясатының мәтіні Kaspersky Security Center жеткізу жиынтығына кіреді. Лицензиялық келісім мен Құпиялылық саясатының ережелерімен келісу, бағдарламаны орнату үшін немесе бағдарламаның алдыңғы нұсқасын жаңарту үшін қажетті шарт болып табылады.

Бағдарламаларды автономды пакеттердің көмегімен орнату

Kaspersky Security Center бағдарламалардың автономды орнату пакеттерін қалыптастыруға мүмкіндік береді. Жеке орнату пакеті, Веб-серверге орналастыруға, пошта арқылы жіберуге немесе клиент құрылғысына басқа тәсілмен жіберуге болатын орындалатын файл болып саналады. Бағдарламаны Kaspersky Security Center қатысуынсыз орнату үшін, алынған файлды клиент құрылғысында жергілікті түрде іске қосуға болады.

Linux жүйесіне арналған автономды желі агентінде nmap утилитасындағы қосымша тәуелділік бар. nmap утилитасы болмаса немесе 6.0 нұсқасынан ертерек болса, Broadcast DHCP Discover функциясына қолдау көрсетілмейді.

Бағдарламаны автономды орнату пакеті арқылы орнату үшін:

1. Қажетті Басқару серверіне қосыңыз.

2. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.

3. Жұмыс аймағында қажетті бағдарламаның орнату пакетін таңдаңыз.

4. Автономды орнату пакетін жасау процесін келесі тәсілдердің көмегімен іске қосыңыз:

   - Орнату пакетінің мәнмәтіндік мәзірінде **Жеке орнату пакетін жасау** тармағын таңдаңыз.
   - Орнату пакетінің жұмыс аймағындағы **Жеке орнату пакетін жасау** сілтемесі бойынша өтіңіз.

   Нәтижесінде, автономды орнату пакетін жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Шебердің соңғы қадамында автономды орнату пакетін клиент құрылғысына жіберу тәсілін таңдаңыз.

5. Бағдарламаның жеке орнату пакетін клиент құрылғысына жіберіңіз.

6. Жеке орнату пакетін клиент құрылғысында іске қосыңыз.

Нәтижесінде, бағдарлама автономды пакетте көрсетілген параметрлері бар клиент құрылғысында орнатылады.

Жасау кезінде, жеке орнату пакеті Веб-серверде автоматты түрде жарияланады. Автономды пакетті жүктеу сілтемесі, жасалған автономды орнату пакеттерінің тізімінде көрсетіледі. Қажет болса, таңдалған автономды пакетті жариялауды болдырмай, оны Веб-серверде қайта жариялауыңызға болады. Әдепкі бойынша, автономды орнату пакеттерін жүктеу үшін 8060 порты қолданылады.

Желілік агенттің орнату пакетінің параметрлері

Желілік агенттің орнату пакетінің параметрлерін конфигурациялау үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.

   Қашықтан орнату қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Желілік агенттің орнату пакетінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

Желілік агенттің орнату пакетінің сипаттары терезесі ашылады.

Жалпы

Жалпы бөлімінде орнату пакеті туралы жалпы ақпарат келтірілген:

- Орнату пакетінің атауы
- Орнату пакеті жасалған бағдарламаның атауы және нұсқасы
- Орнату пакетінің өлшемі
- Орнату пакетін жасау күні
- Орнату пакетін орналастыру қалтасына апаратын жол

Параметрлер

Бұл бөлімде Желілік агент орнатылғаннан кейін, оның жұмысын қамтамасыз ету үшін қажетті параметрлерді конфигурациялауға болады. Осы бөлімнің параметрлері тек Windows басқаратын құрылғылар үшін ғана қолжетімді.

Мақсатты қалта параметрлер блогында Желілік агент орнатылатын клиент құрылғысындағы қалтаны таңдауға болады.

- **Әдепкі қалтаға орнату**

  Осы нұсқа таңдалған болса, Желілік агент <Диск>:\Program Files\Kaspersky Lab\NetworkAgent қалтасына орнатылады. Мұндай қалта болмаса, ол автоматты түрде жасалады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Белгіленген қалтаға орнату**

  Егер бұл нұсқа таңдалса, Желілік агент енгізу өрісінде көрсетілген қалтаға орнатылады.

Төмендегі параметрлер блогында, Желілік агентті қашықтан жою тапсырмасы үшін құпиясөз белгілеуге болады:

- **Жою құпиясөзін пайдалану**

  Параметр қосулы болса, онда **Өзгерту** түймесін басқан кезде бағдарламаны жою үшін құпиясөзді енгізуге болады (тек Windows отбасының операциялық жүйелері басқаратын құрылғылардағы Желілік агент үшін қолжетімді).

  Әдепкі бойынша, параметр өшірулі.

- **Күйі**

  Құпиясөз күйі: **Құпия орнатылды** немесе **Құпиясөз орнатылмаған**.

  Әдепкі бойынша, құпиясөз орнатылмаған.

- **Желілік агент қызметін рұқсатсыз өшіруден немесе тоқтатудан қорғау және параметрлердегі өзгерістердің алдын алу**

  Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, құрамдасты қажетті құқықтарсыз жою немесе өзгерту мүмкін емес. Желілік агенттің жұмысын тоқтату мүмкін емес. Бұл параметр домен контроллерлеріне әсер етпейді.

  Жергілікті әкімші құқықтарымен басқарылатын жұмыс станцияларында Желілік агентті қорғау үшін осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату**

  Бұл параметр қосулы болса, басқару серверіне, желілік агентке, басқару консоліне және iOS MDM серверіне арналған жүктелген барлық жаңартулар мен патчтар автоматты түрде орнатылады.

  Бұл параметр өшірулі болса, жүктелген жаңартулар мен патчтар, олардың күйін *Расталды* деп өзгерткеннен кейін ғана орнатылатын болады. *Анықталмаған* күйі бар жаңартулар мен патчтар орнатылмайды.

  Әдепкі бойынша, параметр қосулы.

Бұл бөлімде Желілік агенттің Басқару серверіне қосылу параметрлерін конфигурациялауға болады. Қосылымды орнату үшін SSL протоколын немесе UDP протоколын пайдалануға болады. Қосылымды орнату үшін келесі параметрлерді көрсетіңіз:

- **Басқару сервері**

  Басқару сервері орнатылған құрылғының мекенжайы.

- **Порт**

  Қосылым орындалатын порт нөмірі.

- **SSL порты**

  SSL протоколының көмегімен қосылым орындалатын порт нөмірі.

- **Сервер сертификатын пайдалану**

  Егер бұл параметр қосулы болса, Желілік агенттің Басқару серверіне қатынасуын түпнұсқалық растамадан өткізу үшін **Шолу** түймесін басқан кезде көрсетуге болатын сертификат файлы пайдаланылады.

  Егер бұл параметр өшірулі болса, сертификат файлы, Желілік агентті **Сервер мекенжайы** өрісінде көрсетілген мекенжайға алғаш қосқан кезде Басқару серверінен алынады.

  Параметрді өшіру ұсынылмайды, себебі Серверге қосылған кезде Желілік агентпен Басқару серверінің сертификатын автоматты түрде алу қауіпсіз емес болып табылады.

  Әдепкі бойынша, жалауша қойылған.

- **SSL пайдалану**

  Бұл параметр қосулы болса, Басқару серверіне қосылу SSL протоколының көмегімен, қорғалған порт арқылы орындалатын болады.

  Әдепкі бойынша, параметр өшірулі. Сіздің қосылымыңыз қауіпсіз болып қала беруі үшін, бұл параметрді өшірмеу ұсынылады.

- **UDP портын пайдалану**

  Егер бұл параметр қосулы болса, Желілік агентінің Басқару серверіне қосылуы UDP порты арқылы жүзеге асырылады. Бұл, клиент құрылғыларын басқаруға және олар туралы ақпарат алуға мүмкіндік береді.

  UDP порты Желілік агент орнатылған басқарылатын құрылғыларда ашық болуы керек. Сондықтан бұл параметрді өшірмеу ұсынылады.

  Әдепкі бойынша, параметр қосулы.

- **UDP портының нөмірі**

  Өрісте Басқару серверін UDP протоколы бойынша Желілік агентке қосу портының нөмірін көрсетуге болады.

  Әдепкі бойынша, UDP портының нөмірі – 15000.

- **Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу**

  Параметр қосылса, Желілік агент пайдаланатын порттар Microsoft Windows брандмауэрінің ерекшеліктер тізіміне қосылады.

  Әдепкі бойынша, параметр қосулы.

- **Прокси-серверді пайдалану**

  Бұл параметр қосылса, прокси сервер параметрлерін көрсетіңіз:

  - **Прокси-сервердің мекенжайы**
  - **Прокси-сервердің порты**

  Егер сіздің прокси серверіңіз аутентификацияны қажет етсе, **Прокси-сервердегі түпнұсқалық растама** параметрін қосыңыз және прокси серверге қосылым орнатылған тіркелгінің **Пайдаланушы аты** мен **Құпиясөз** көрсетіңіз. Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

Үйлесімділік себептері бойынша Желілік агент орнату пакетінің параметрлерінде прокси-серверге қосылу параметрлерін көрсету ұсынылмайды.

Қосымша

Кеңейтілген бөлімінде қосылым шлюзін қалай қолдануға болатынын конфигурациялауға болады. Бұл үшін келесі әрекеттерді орындауға болады:

- Желілік агентті, деректер жіберу уақытында Басқару серверіне қосылу, онымен байланысу және деректерді Желілік агентте қауіпсіз жерде сақтау үшін демилитаризацияланған аймақтағы қосылым шлюзі (DMZ) ретінде қолданыңыз.

- Басқару серверіне қосылу санын азайту үшін Басқару серверіне қосылым шлюзі арқылы қосылыңыз. Бұл жағдайда, қосылым шлюзі ретінде қолданылатын құрылғының мекенжайын **Қосылым шлюзі мекенжайы** өрісіне енгізіңіз.

- Желіңізде виртуалды машиналар болса, Virtual Desktop Infrastructure (VDI) үшін қосылымды конфигурациялаңыз. Бұл үшін келесі әрекеттерді орындаңыз:

  - **VDI үшін динамикалық режимді қосу**

    Параметр қосулы болса, виртуалды машинада орнатылған Желілік агент үшін Virtual Desktop Infrastructure (VDI) үшін динамикалық режим қосылады.

    Әдепкі бойынша, параметр өшірулі.

  - **VDI параметрлерін оңтайландыру**

    Егер параметр қосулы болса, Желілік агенттің параметрлерінде келесі функциялар өшіріледі:

    - Орнатылған бағдарламалық жасақтама туралы ақпарат алу
    - Аппараттық жасақтама туралы ақпарат алу
    - Осалдықтардың болуы туралы ақпарат алу
    - Қажетті жаңартулар туралы ақпарат алу

    Әдепкі бойынша, параметр өшірулі.

- **Желілік агентті орнатқаннан кейін пайдаланушыны тіркеу утилитасын іске қосуға рұқсат беру**

  Бұл опция қосылса, желілік агент орнатылғаннан кейін, пайдаланушыны құрылғы иесі ретінде тіркеу утилитасы іске қосылады. Әдепкі бойынша, параметр өшірулі.

Қосымша құрамдастар

Бұл бөлімде Желілік агентпен бірге орнатылатын қосымша құрамдастарды таңдауға болады.

Тегтер

Тегтер бөлімінде клиент құрылғыларына Желілік агентті орнатқаннан кейін, оларға қосуға болатын кілт сөздер (тегтер) тізімі көрсетіледі. Сіз тізімдегі тегтерді қоса аласыз және жоя аласыз, сондай-ақ атауын өзгерте аласыз.

Тегтің жанында жалауша қойылған болса, онда тег, басқарылатын құрылғыларға Желілік агентті орнату кезінде автоматты түрде қосылады.

Тегтің жанындағы жалауша алынып тасталса, онда тег, басқарылатын құрылғыларға Желілік агентті орнату кезінде автоматты түрде қосылмайды. Бұл тегті құрылғыларға қолмен қосуға болады.

Тегті тізімнен алып тастаған кезде, тег қосылған барлық құрылғылардан автоматты түрде алынады.

Тексерістер журналы

Бұл бөлімде орнату пакетінің тексерістер журналын қарап шығуға болады. Сіз тексерулерді салыстыра аласыз, тексерулерді қарап шыға аласыз, тексерулерді файлға сақтай аласыз, тексерулердің сипаттамасын қоса аласыз және өзгерте аласыз.

Желілік агенттің орнату пакетінің параметрлері, төмендегі кестеде келтірілген нақты операциялық жүйе үшін қолжетімді.

Желілік агенттің орнату пакетінің параметрлері

Сипаттар бөлімі	Windows	Mac	Linux
Жалпы	✓	✓	✓
Параметрлер	✓	—	—
Қосылым	✓	✓ (**Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу** және **Тек прокси-серверді автоматты түрде анықтауды пайдалану** параметрлерінен бөлек)	✓ (**Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу** және **Тек прокси-серверді автоматты түрде анықтауды пайдалану** параметрлерінен бөлек)
Кеңейтілген	✓	✓	✓
Қосымша құрамдастар	✓	✓	✓
Тегтер	✓	✓ (автоматты түрде тег қою ережелерінен бөлек)	✓ (автоматты түрде тег қою ережелерінен бөлек)
Тексерістер журналы	✓	✓	✓

Құпиялылық саясатын қарау

Құпиялық саясаты интернетте https://www.kaspersky.ru/products-and-services-privacy-policy бетінде қолжетімді; сондай-ақ, ол офлайн-режимде де қолжетімді. Сіз Құпиялылық саясатымен таныса аласыз, мысалы, Желілік агентті орнатпас бұрын.

Құпиялылық саясатын офлайн-режимде оқу үшін:

1. Kaspersky Security Center орнатушысын іске қосыңыз.
2. Орнатушы терезесінде **Орнату пакеттерін шығарып алу** сілтемесі бойынша өтіңіз.
3. Ашылған тізімнен Kaspersky Security Center Желілік агентін таңдап, **Келесі** түймесін басыңыз.

   privacy_policy.txt файлы құрылғыңызда, сіз көрсеткен қалтада, NetAgent ішкі қалтасында пайда болады.

Ұялы құрылғыларды басқару жүйелерін орналастыру

Бұл бөлімде iOS MDM және Kaspersky Endpoint Security протоколдары бойынша Ұялы құрылғыларды басқару жүйелерінің орналастырылуы сипатталған.

iOS MDM протоколы бойынша басқару жүйесін орналастыру

Kaspersky Security Center қызметі iOS негізіндегі мобильдік құрылғыларды басқаруға мүмкіндік береді. iOS MDM құрылғылары — iOS MDM серверіне қосылған, басқару сервері арқылы басқарылатын iOS мобильдік құрылғылары.

Ұялы құрылғыларды iOS MDM серверіне қосу келесі ретпен жүзеге асырылады:

1. Әкімші iOS MDM серверін орнатады
2. Әкімші Apple Push Notification Service (APNs) сертификатын алады (APNs сертификатын алу, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   APNs сертификаты Басқару серверіне iOS MDM құрылғыларына push хабарландыруларын жіберу үшін APNs серверіне қосылуға мүмкіндік береді.
3. Әкімші iOS MDM серверінде APNs сертификатын орнатады.
4. Әкімші iOS мобильдік құрылғысының пайдаланушысы үшін iOS MDM профилін жасайды.

   iOS MDM профилінде iOS ұялы құрылғыларын Басқару серверіне қосуға арналған параметрлердің жиынтығы бар.

Профильді орнатқаннан және iOS MDM мобильді құрылғысын Басқару серверімен синхрондағаннан кейін, құрылғы консоль ағашының **Мобильді құрылғыларды басқару** қалтасында кірістірілген **Мобильді құрылғылар** қалтасында көрсетіледі.

iOS MDM серверін орнату

iOS MDM серверін жергілікті құрылғыға орнату үшін:

1. setup.exe орындалатын файлын іске қосыңыз.

   Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады.

iOS MDM серверін орнату сілтемесі арқылы бағдарламалар таңдауы бар терезеде iOS MDM серверін орнату шеберін іске қосыңыз.

2. Мақсатты қалтаны таңдаңыз.

   Әдепкі бойынша мақсатты қалта: <Диск>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Мұндай қалта болмаса, ол орнату барысында автоматты түрде жасалады. Сіз мақсатты қалтаны **Шолу** түймесі арқылы өзгерте аласыз.

3. Шебердің **iOS MDM серверіне қосылу параметрлерін көрсету** терезесінде, **iOS MDM қызметіне қосылудың сыртқы порты** өрісінде ұялы құрылғыларды iOS MDM қызметіне қосуға арналған сыртқы портты көрсетіңіз.

   Ұялы құрылғылар 5223 сыртқы портын APNs серверімен байланысу үшін пайдаланады. Желілік экранда 17.0.0.0/8 мекенжайлар ауқымына қосылу үшін 5223-порт ашық екеніне көз жеткізіңіз.

   Құрылғыны iOS MDM серверіне қосу үшін әдепкі бойынша 443-порт қолданылады. Егер 443-портты басқа сервис немесе қолданба пайдаланып жатса, оны, мысалы, 9443-портқа өзгертуге болады.

   iOS MDM сервері APNs серверіне хабарландырулар жіберу үшін 2197 сыртқы портын пайдаланады.

   APNs серверлері теңдестірілген жүктеме режимінде жұмыс істейді. Ұялы құрылғылар хабарландыру алу үшін әрқашан бірдей IP мекенжайларына қосылмайды. 17.0.0.0/8 мекенжайлар ауқымы Apple компаниясына тағайындалған, сондықтан бұл ауқымды желілік экран параметрлерінде рұқсат етілген деп көрсету ұсынылады.

4. Бағдарлама құрамдастары арасында өзара әрекеттесу үшін порттарды қолмен конфигурациялағыңыз келсе, **Жергілікті порттарды қолмен орнату** параметрін таңдап, келесі параметрлердің мәндерін көрсетіңіз:

   - **Желілік агентке қосылу порты**. Өрісте iOS MDM қызметін Желілік агентке қосу портын көрсетіңіз. Әдепкі бойынша 9799-порт орнатылған.
   - **iOS MDM қызметіне қосылудың жергілікті порты**. Өрісте Желілік агентті iOS MDM қызметіне қосу портын көрсетіңіз. Әдепкі бойынша 9899-порт орнатылған.

   Әдепкі бойынша мәндерді пайдалану ұсынылады.

5. Шебердің **Ұялы құрылғылар серверінің сыртқы мекенжайы** терезесінде, **Ұялы құрылғылар серверіне қашықтан қосылу веб-мекенжайы** өрісінде iOS MDM сервері орнатылатын клиент құрылғысы мекенжайын көрсетіңіз.

   Бұл мекенжай басқарылатын ұялы құрылғыларды iOS MDM қызметіне қосу үшін қолданылады. Клиент құрылғысы, оған iOS MDM құрылғыларын қосу үшін қолжетімді болуы керек.

   Клиент құрылғысының мекенжайын келесі пішімдердің бірінде көрсетуге болады:

   - Құрылғының FQDN атауы (мысалы, mdm.example.com)
   - Құрылғының NetBIOS атауы

   Мекенжайы бар жолға URL схемасын және порт нөмірін қосуға болмайды: бұл мәндер автоматты түрде қосылады.

Шебер жұмысының нәтижесінде iOS MDM сервері жергілікті құрылғыға орнатылады. iOS MDM сервері консоль ағашының **Ұялы құрылғыларды басқару** қалтасында көрсетіледі.

iOS MDM серверін тыныш режимде орнату

Kaspersky Security Center бағдарламасы iOS MDM серверін жергілікті құрылғыға тыныш режимде, яғни орнату параметрлерін интерактивті түрде енгізбей орнатуға мүмкіндік береді.

iOS MDM серверін жергілікті құрылғыға тыныш режимде орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімді оқып шықсаңыз және оның шарттарын қабылдасаңыз, төмендегі пәрменді қолданыңыз.

2. Келесі пәрменді орындаңыз:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 < setup_parameters >"
   ```

   мұндағы `setup_parameters` – бір-бірінен бос орын арқылы бөлінген параметрлер мен олардың мәндерінің тізбесі (`PROP1=PROP1VAL PROP2=PROP2VAL`). Setup.exe файлы Kaspersky Security Center дистрибутивінің ішіндегі Server қалтасында орналасқан.

iOS MDM серверін тыныш режимде орнату кезінде қолдануға болатын параметрлердің аттары мен ықтимал мәндері төмендегі кестеде келтірілген. Параметрлерді кез келген тәртіпте көрсетуге болады.

iOS MDM серверін тыныш режимде орнату параметрлері

Параметрдің атауы	Параметрдің сипаттамасы	Қолжетімді мәндері
EULA	Лицензиялық келісімнің шарттарымен келісу. Бұл параметр міндетті болып саналады.	• 1 – Мен Лицензиялық келісімді толығымен оқып шыққанымды және оның шарттарын қабылдайтынымды растаймын. • Басқа мән немесе белгіленбеген – Лицензиялық келісімнің шарттарымен келіспейсіз (орнату жүзеге асырылмайды).
DONT_USE_ANSWER_FILE	iOS MDM серверін орнату параметрі бар xml-файлды қолдану керек пе, керек емес пе. xml-файл орнату пакеті бар жиынтықпен бірге жеткізіледі немесе Басқару серверінде бар. Файлға апаратын қосымша жолды көрсетудің қажеті жоқ. Бұл параметр міндетті болып саналады.	• 1 – параметрлері бар XML-файлды қолданбау. • Басқа мән немесе белгіленбеген – параметрлері бар XML-файлды қолдану.
INSTALLDIR	iOS MDM серверін орнату қалтасы. Бұл параметр міндетті емес.	Жол мәні, мысалы, `INSTALLDIR=\"C:\install\"`.
CONNECTORPORT	iOS MDM қызметін Желілік агентке қосудың жергілікті порты. Әдепкі бойынша 9799-порт орнатылған. Бұл параметр міндетті емес.	Сандық мән.
LOCALSERVERPORT	Желілік агентті iOS MDM қызметіне қосудың жергілікті порты. Әдепкі бойынша 9899-порт орнатылған. Бұл параметр міндетті емес.	Сандық мән.
EXTERNALSERVERPORT	Құрылғыны iOS MDM серверіне қосуға арналған порт. Әдепкі бойынша 443-порт орнатылған. Бұл параметр міндетті емес.	Сандық мән.
EXTERNAL_SERVER_URL	iOS MDM сервері орнатылатын клиент құрылғысының сыртқы мекенжайы. Бұл мекенжай басқарылатын ұялы құрылғыларды iOS MDM қызметіне қосу үшін қолданылады. Клиент құрылғысы, оған iOS MDM қызметін қосу үшін қолжетімді болуы тиіс. Мекенжайға URL схемасы мен порт нөмірі кірмеуі тиіс, себебі бұл мәндер автоматты түрде қосылады. Бұл параметр міндетті емес.	• Құрылғының FQDN атауы (мысалы, mdm.example.com) • Құрылғының NetBIOS атауы • Құрылғының IP мекенжайы

Параметрдің атауы	Параметрдің сипаттамасы	Қолжетімді мәндері
WORKFOLDER	iOS MDM серверінің жұмыс қалтасы. Жұмыс қалтасы көрсетілмесе, әдепкі бойынша деректер қалтаға жазылады. Бұл параметр міндетті емес.	Жол мәні, мысалы, `WORKFOLDER=\"C:\work\"`.
MTNCY	iOS MDM серверін бірнеше виртуалды Серверлермен бірге қолдану. Бұл параметр міндетті емес.	• 1 – iOS MDM серверін бірнеше виртуалды Басқару сервері қолданады. • Басқа мән немесе белгіленбеген – iOS MDM серверін бірнеше виртуалды Басқару сервері қолданбайды.

Мысалы:
```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

iOS MDM серверін орнату параметрлері "iOS MDM серверін орнату" бөлімінде толық сипатталған.

iOS MDM серверін орналастыру схемалары

iOS MDM серверінің орнатылған көшірмелерінің саны қолжетімді аппараттық жасақтаманың болуына байланысты, сондай-ақ қызмет көрсетілетін ұялы құрылғылардың жалпы санына байланысты таңдалуы мүмкін.

Kaspersky Device Management for iOS қолданбасын бір рет орнатуға 50 000-нан аспайтын ұялы құрылғылар ұсынылатынын ескеру керек. Жүктемені азайту үшін барлық көптеген құрылғыларды iOS MDM сервері орнатылған бірнеше серверлер арасында бөлуге болады.

iOS MDM құрылғыларының түпнұсқалық растамасы пайдаланушы сертификаттарының көмегімен жүзеге асырылады (құрылғыға орнатылған профильде ол тиесілі пайдаланушының сертификаты бар). Сондықтан, iOS MDM серверін орналастырудың екі схемасы мүмкін:

- Жеңілдетілген схема
- Kerberos Constrained Delegation (KCD) мәжбүрлеп табыстауын қолдана отырып орналастыру схемасы

Жеңілдетілген орналастыру схемасы

iOS MDM серверін жеңілдетілген схема бойынша орналастырған кезде ұялы құрылғылар iOS MDM веб-қызметіне тікелей қосылады. Бұл ретте, құрылғылардың түпнұсқалық растамасы үшін Басқару сервері шығарған пайдаланушы сертификаттары ғана пайдаланылуы мүмкін. Пайдаланушы сертификаттары үшін жалпыға ортақ кілт инфрақұрылымымен (Public Key Infrastructure, PKI) біріктіру мүмкін емес.

Kerberos Constrained Delegation (KCD) мәжбүрлеп табыстауын қолдана отырып орналастыру схемасы

Kerberos шектелген делегацияны (KCD) енгізу схемасын пайдалану үшін келесі талаптарды орындау қажет:

- Басқару сервері және iOS MDM сервері ұйымның ішкі желісінде орналасқан.
- KCD қолдауы бар кері прокси-сервер пайдаланылады.

Бұл орналастыру схемасы мыналарды қамтиды:

- KCD қолдайтын кері прокси-сервермен интеграция;
- ұялы құрылғылар түпнұсқалық растамасы үшін Kerberos Constrained Delegation мәжбүрлеп табыстауды пайдалану;
- пайдаланушы сертификаттарын пайдалану үшін жалпыға ортақ кілт инфрақұрылымымен (PKI) біріктіру.

Осы орналастыру схемасын пайдалану кезінде мыналарды ескеру қажет:

- Басқару консолінде iOS MDM веб-қызметінің параметрлерінде **Kerberos Constrained Delegation әдісімен үйлесімділікті қамтамасыз ету** жалаушасын қою керек.
- iOS MDM веб-қызметінің сертификаты ретінде кері прокси-серверде жариялау кезінде TMG-де берілген арнайы (кастомизацияланған) сертификат көрсетілуі керек.
- iOS құрылғыларына арналған пайдаланушы сертификаттарын Домендік сертификаттау орталығы (Certification authority, бұдан әрі CA) шығаруы керек. Егер доменде бірнеше түбірлік CA болса, онда кері прокси-серверде iOS MDM веб-қызметін жариялау кезінде көрсетілген CA пайдаланушы сертификаттары шығарылуы керек.

  Пайдаланушы сертификатының көрсетілген талапқа сәйкестігі бірнеше тәсілмен қамтамасыз етілуі мүмкін:

  - iOS MDM профилін құру шеберінде және сертификаттарды орнату шеберінде пайдаланушы сертификатын көрсету.
  - Басқару серверін домендік PKI инфрақұрылымымен біріктіру және сертификаттарды шығару ережелерінде тиісті параметрді конфигурациялау:

    1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Сертификаттар** салынған қалтасын таңдаңыз.
    2. **Сертификаттар** қалтасының жұмыс аймағында, **Сертификат беру ережелерін конфигурациялау** түймесі арқылы **Сертификаттарды шығару ережелері** терезесін ашыңыз.
    3. **PKI жүйесімен интеграциялау** бөлімінде жалпыға ортақ кілт инфрақұрылымымен біріктіруді конфигурациялаңыз.
    4. **Ұялы құрылғы сертификаттарын шығару** бөлімінде сертификаттар көзін көрсетіңіз.

Келесі болжамдармен KCD шектеулі табыстау конфигурациясы мысалын қарастырайық:

- iOS MDM веб-қызметі 443-портта іске қосылған;
- кері прокси-серверден құрылғы атауы – firewall.mydom.local;
- iOS MDM веб-қызметі бар құрылғы атауы – iosmdm.mydom.local.
- iOS MDM веб-қызметінің сыртқы жарияланымының атауы – iosmdm.mydom.global.

http/iosmdm.mydom.local үшін Service Principal Name

Доменде iOS MDM (iosmdm.mydom.local) веб-қызметі бар құрылғы үшін Service Principal Name (SPN) жазу қажет:

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Кері прокси-сервері бар құрылғылардың домен сипаттарын конфигурациялау (firewall.mydom.local)

Трафикті табыстау үшін кері прокси-сервері (firewall.mydom.local) бар құрылғыны SPN (http/iosmdm.mydom.local) бойынша анықталған қызметке сеніп тапсыруға болады.

Кері прокси-сервері бар құрылғыны SPN (http/iosmdm.mydom.local) бойынша анықталған қызметке сеніп тапсыру үшін, әкімші келесі әрекеттерді орындауы тиіс:

1. Microsoft Management Console "Active Directory Users and Computers" жабдықтарында кері прокси-сервері (firewall.mydom.local) орнатылған құрылғыны таңдаңыз.

2. **Delegation** қойыншасындағы құрылғының сипаттарында **Trust this computer for delegation to specified service only** қосқышы үшін **Use any authentication protocol** нұсқасын таңдау.

3. **Services to which this account can present delegated credentials** тізіміне SPN http/iosmdm.mydom.local қосу.

Жарияланатын веб-қызмет (iosmdm.mydom.global) үшін айрықша (кастомизацияланған) сертификат

FQDN iosmdm.mydom.global бойынша орналасқан iOS MDM веб-қызметі үшін айрықша (кастомизацияланған) сертификатты шығару және оны Басқару консоліндегі iOS MDM веб-қызметі параметрлерінде әдепкі бойынша сертификат орнына көрсету керек.

Сертификаты бар контейнерде (p12 немесе pfx кеңейтімі бар файл) түбірлік сертификаттар тізбегі (жария бөліктер) болуы керек екенін де ескеру қажет.

iOS MDM веб-қызметінің кері прокси-сервердегі жарияланымдары

Кері прокси-серверде ұялы құрылғы тарапынан iosmdm.mydom.global атты 443-портқа баратын трафик үшін, FQDN iosmdm.mydom.global атауына арнап шығарылған сертификатты қолдану арқылы SPN http/iosmdm.mydom.local мекенжайына KCD конфигурациялау керек. Жарияланымда да, жарияланатын веб-қызметте де бірдей серверлік сертификат болуы керек екенін ескеру қажет.

APNs сертификатын алу

APNs сертификатыңыз бұрыннан бар болса, жаңасын жасаудың орнына, оны жаңартыңыз. APNs сертификатын жаңадан жасалған сертификатқа ауыстыру кезінде, Басқару сервері қазіргі сәтте қосылған iOS ұялы құрылғыларын басқара алмай қалады.

Сертификатқа қол қоюды сұрауды (бұдан әрі - CSR сұрауы) жасау үшін, APNs сертификатын алу шеберінің бірінші қадамында болашақ сертификаттың жеке бөлігі (private key) құрылғының жедел жадында сақталады. Сол себепті, шебердің барлық қадамдары бағдарламамен жұмыстың бір сессиясы шеңберінде аяқталуы тиіс.

APNs сертификатын алу үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.

2. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.

3. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   iOS MDM сервері сипаттары терезесі ашылады.

4. iOS MDM сервері сипаттары терезесінде **Сертификаттар** бөлімін таңдаңыз.

5. **Сертификаттар** бөлімінде, **Apple push-хабарландыруының сертификаты** параметрлері блогында **Жаңасын сұрау** түймесін басыңыз.

   APNs сертификатын алу шебері іске қосылып, **Жаңасын сұрау** терезесі ашылады.

6. Сертификатқа қол қоюды сұрауын (бұдан әрі CSR сұрауы) жасаңыз. Бұл үшін келесі әрекеттерді орындаңыз:

   a. **CSR жасау** түймесін басыңыз.

   b. Ашылған **CSR жасау** терезесінде сұраудың атауын, компания мен департамент атауын, қаланы, облысты және елді көрсетіңіз.

   c. **Сақтау** түймесін басып, CSR сұрауы сақталатын файл атауын көрсетіңіз.

   Болашақ сертификаттың жеке бөлігі (private key) құрылғының жадында сақталады.

7. CSR сұрауымен бірге жасалған файлды сіздің CompanyAccount арқылы Kaspersky бағдарламасына қол қою жіберіңіз.

   > CSR сұрауына қол қою, Ұялы құрылғыларды басқаруды қолдануға рұқсат беретін кілтті CompanyAccount порталына жүктегеннен кейін ғана қолжетімді.

   Электрондық сұрауыңыз өңделгеннен кейін, сіз Kaspersky қол қойған CSR сұрауы файлын аласыз.

8. Қол қойылған CSR сұрауы файлын ерікті Apple ID арқылы Apple Inc. веб-сайтына жіберіңіз.

   > Дербес Apple ID қолдану ұсынылмайды. Бөлек Apple ID жасап, оны корпоративтік идентификатор ретінде қолданыңыз. Жасалған Apple ID-ді жекелеген қызметкердің емес, ұйымның пошта жәшігіне байлаңыз.

   CSR сұрауыңыз Apple Inc. тарапынан өңделгеннен кейін, сіз APNs сертификатының жария бөлігін алатын боласыз. Алынған файлды дискіге сақтаңыз.

9. APNs сертификатын CSR сұрауын қалыптастыру кезінде жасалған жеке кілтпен бірге PFX пішіміндегі файлға экспорттаңыз. Бұл үшін келесі әрекеттерді орындаңыз:

   a. **Жаңа APNs сертификатын сұрау** терезесінде **CSR аяқтау** түймесін басыңыз.

   b. Ашылған **Ашу** терезесінде, CSR сұрауы Apple Inc. тарапынан өңделгеннен кейін алынған сертификаттың жария бөлігімен бірге файлды таңдап, **Ашу** түймесін басыңыз.

      Сертификатты экспорттау іске қосылады.

   c. Ашылған терезеде жеке кілтке арналған құпиясөзді енгізіп, **OK** түймесін басыңыз.

      Белгіленген құпиясөз APNs сертификатын iOS MDM серверіне орнату үшін қолданылады.

   d. Ашылған **APNs сертификатын сақтау** терезесінде APNs сертификатын сақтауға арналған файл атауын көрсетіп, ол сақталатын қалтаны таңдап, **Сақтау** түймесін басыңыз.

Сертификаттың жеке және жария бөліктері біріктіріледі, APNs сертификаты PFX пішіміндегі файлға сақталады. Содан кейін, сіз iOS MDM серверіне APNs сертификатын орната аласыз.

APNs сертификатын жаңарту

APNs сертификатын жаңарту үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.

2. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.

3. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   iOS MDM сервері сипаттары терезесі ашылады.

4. iOS MDM сервері сипаттары терезесінде **Сертификаттар** бөлімін таңдаңыз.

5. **Сертификаттар** бөлімінде, **Apple push-хабарландыруының сертификаты** параметрлері блогында **Жаңалау** түймесін басыңыз.

   APNs сертификатын жаңарту шебері іске қосылып, **APNs сертификатын жаңарту** терезесі ашылады.

6. Сертификатқа қол қоюды сұрауын (бұдан әрі CSR сұрауы) жасаңыз. Бұл үшін келесі әрекеттерді орындаңыз:

   a. **CSR жасау** түймесін басыңыз.

   b. Ашылған **CSR жасау** терезесінде сұраудың атауын, компания мен департамент атауын, қаланы, облысты және елді көрсетіңіз.

   c. **Сақтау** түймесін басып, CSR сұрауы сақталатын файл атауын көрсетіңіз.

   Болашақ сертификаттың жеке бөлігі (private key) құрылғының жадында сақталады.

7. CSR сұрауымен бірге жасалған файлды сіздің CompanyAccount арқылы Kaspersky бағдарламасына қол қою жіберіңіз.

   > CSR сұрауына қол қою, Ұялы құрылғыларды басқаруды қолдануға рұқсат беретін кілтті CompanyAccount порталына жүктегеннен кейін ғана қолжетімді.

   Электрондық сұрауыңыз өңделгеннен кейін, сіз Kaspersky қол қойған CSR сұрауы файлын аласыз.

8. Қол қойылған CSR сұрауы файлын ерікті Apple ID арқылы Apple Inc. веб-сайтына жіберіңіз.

   > Дербес Apple ID қолдану ұсынылмайды. Бөлек Apple ID жасап, оны корпоративтік идентификатор ретінде қолданыңыз. Жасалған Apple ID-ді жекелеген қызметкердің емес, ұйымның пошта жәшігіне байлаңыз.

   CSR сұрауыңыз Apple Inc. тарапынан өңделгеннен кейін, сіз APNs сертификатының жария бөлігін алатын боласыз. Алынған файлды дискіге сақтаңыз.

9. Сертификаттың жария бөлігін сұраңыз. Бұл үшін келесі әрекеттерді орындаңыз:

   a. Apple Push Certificates порталына өтіңіз. Порталда авторизациядан өту үшін сертификатты бастапқы сұрау кезінде алынған Apple ID керек болады.

   b. Сертификаттар тізімінен, APSP атауы ("APSP: <нөмір>" пішіміндегі атауы) iOS MDM сервері қолданатын сертификаттың APSP атауына сай келетін сертификатты таңдап, **Жаңалау** түймесін басыңыз.

      APNs сертификаты жаңартылады.

   c. Портал жасаған сертификатты сақтап қойыңыз.

10. APNs сертификатын CSR сұрауын қалыптастыру кезінде жасалған жеке кілтпен бірге PFX пішіміндегі файлға экспорттаңыз. Бұл үшін келесі әрекеттерді орындаңыз:

    a. **APNs сертификатын жаңарту** терезесінде **CSR аяқтау** түймесін басыңыз.

    b. Ашылған **Ашу** терезесінде, CSR сұрауы Apple Inc. тарапынан өңделгеннен кейін алынған сертификаттың жария бөлігімен бірге файлды таңдап, **Ашу** түймесін басыңыз.

       Сертификатты экспорттау іске қосылады.

    c. Ашылған терезеде жеке кілтке арналған құпиясөзді енгізіп, **OK** түймесін басыңыз.

       Белгіленген құпиясөз APNs сертификатын iOS MDM серверіне орнату үшін қолданылады.

    d. Ашылған **APNs сертификатын жаңарту** терезесінде APNs сертификатын сақтауға арналған файл атауын көрсетіп, ол сақталатын қалтаны таңдап, **Сақтау** түймесін басыңыз.

Сертификаттың жеке және жария бөліктері біріктіріледі, APNs сертификаты PFX пішіміндегі файлға сақталады.

iOS MDM серверінің резервтік сертификатын конфигурациялау

iOS MDM сервері функционалдылығы резервтік сертификатты жазып беруге мүмкіндік береді. Бұл сертификат, iOS MDM серверінің сертификатының әрекет ету мерзімі өтіп кеткеннен кейін басқарылатын iOS құрылғыларын ауыстырып қосуды қамтамасыз ету үшін iOS MDM профильдерінде қолданылуға арналған.

Егер сіздің iOS MDM серверіңіз әдепкі бойынша Kaspersky берген сертификатты қолданса, сіз iOS MDM сервері сертификатының мерзімі аяқталғанға дейін резервтік сертификат шығара аласыз (немесе өз сертификатыңызды резервтік сертификат ретінде көрсете аласыз). Әдепкі бойынша, резервтік сертификат iOS MDM сервері сертификатының жарамдылық мерзімі аяқталғанға дейін 60 күн бұрын автоматты түрде шығарылады. iOS MDM серверінің резервтік сертификаты iOS MDM сервері сертификатының жарамдылық мерзімі аяқталғаннан кейін бірден негізгі сертификатқа айналады. Жалпыға ортақ кілт барлық басқарылатын құрылғыларға конфигурациялық профильдер арқылы таралады, сондықтан сізге оны қолмен берудің қажеті жоқ.

iOS MDM серверінің резервтік сертификатын шығару немесе пайдаланушы резервтік сертификатын көрсету үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.

2. Ұялы құрылғылар серверлері тізімінде тиісті iOS MDM серверін таңдаңыз және оң жақ тақтада **iOS MDM серверін конфигурациялау** түймесін басыңыз.

3. Ашылған iOS MDM сервері сипаттары терезесінде **Сертификаттар** бөлімін таңдаңыз.

4. **Резервтік сертификат** параметрлер блогында келесі әрекеттердің бірін орындаңыз:

   - Өздігінен қол қойылған сертификатты одан әрі қолдануды жоспарласаңыз (яғни Kaspersky шығарған):

     a. **Мәселе** түймесін басыңыз.

     b. Ашылған **Белсендіру күні** терезесінде, резервтік сертификатты қолдану қажет күннің екі нұсқасының бірін таңдаңыз:

        - Резервтік сертификатты ағымдағы сертификатың жарамдылық мерзімі өтіп кеткен сәтте қолданғыңыз келсе, **Ағымдағы сертификаттың мерзімі біткен кезде** параметрін таңдаңыз.

        - Резервтік сертификатты ағымдағы сертификаттың жарамдылық мерзімінің өтіп кетуіне дейін қолданғыңыз келсе, **Белгіленген мерзімнен (күндерден) кейін** параметрін таңдаңыз. Осы параметрдің жанындағы енгізу өрісінде резервтік сертификат ағымдағы сертификатты ауыстыруы керек кезеңнің ұзақтығын көрсетіңіз.

        > Сіз көрсеткен резервтік сертификаттың жарамдылық мерзімі iOS MDM серверінің ағымдағы сертификатының жарамдылық мерзімінен аспауы керек.

     c. **OK** түймесін басыңыз.

     iOS MDM серверінің резервтік сертификаты шығарылды.

   - Сенімді сертификаттау орталығы шығарған пайдаланушы сертификатын пайдалануды жоспарласаңыз:

     a. **Қосу** түймесін басыңыз.

     b. Ашылған Жетектеуші терезесінде, құрылғыңызда сақталған PEM, PFX немесе P12 пішіміндегі сертификат файлын көрсетіп, **Ашу** түймесін басыңыз.

     Пайдаланушы сертификаты iOS MDM серверінің резервтік сертификаты ретінде көрсетілген.

iOS MDM серверінің резервтік сертификаты көрсетілді. Резервтік сертификат туралы толық ақпарат **Резервтік сертификат** параметрлер блогында көрсетіледі (сертификаттың атауы, сертификат шығарушының атауы, резервтік сертификаттың жарамдылық мерзімі және қолданылу күні, егер бар болса).

APNs сертификатын iOS MDM серверіне орнату

APNs сертификатын алғаннан кейін, APNs сертификатын iOS MDM серверіне орнату қажет.

APNs сертификатын iOS MDM серверіне орнату үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.

2. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.

3. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   iOS MDM сервері сипаттары терезесі ашылады.

4. iOS MDM сервері сипаттары терезесінде **Сертификаттар** бөлімін таңдаңыз.

5. **Сертификаттар** бөлімінде, **Apple push-хабарландыруының сертификаты** параметрлері блогында **Орнату** түймесін басыңыз.

6. APNs сертификаты бар PFX пішіміндегі файлды таңдаңыз.

7. APNs сертификатын экспорттау кезінде көрсетілген жеке кілттің құпиясөзін енгізіңіз.

Нәтижесінде, APNs сертификаты iOS MDM серверіне орнатылады. Сертификат туралы ақпарат **Сертификаттар** бөліміндегі iOS MDM серверінің сипаттары терезесінде көрсетіледі.

Apple Push Notification сервисіне қатынасты конфигурациялау

iOS MDM веб-қызметінің дұрыс жұмыс істеуі үшін, сондай-ақ ұялы құрылғылар әкімшінің пәрмендеріне уақтылы жауап беруін қамтамасыз ету үшін, iOS MDM серверінің параметрлерінде Apple Push Notification Service сертификатын (бұдан әрі - APNs сертификаты) көрсету қажет.

Apple Push Notification (бұдан әрі - APNs) сервисімен өзара әрекеттесе отырып, iOS MDM веб-қызметі api.push.apple.com сыртқы мекенжайына 2197-порт (шығыс) арқылы қосылады. Сондықтан, iOS MDM веб-қызметіне 17.0.0.0/8 мекенжайлар ауқымы үшін TCP 2197 портына қатынасу мүмкіндігін ұсыну керек. iOS құрылғысы тарапынан – 17.0.0.0/8 мекенжайлар ауқымы үшін TCP 5223 портына қатынасу.

Егер iOS MDM веб-қызметі тарапынан APNs сервисіне қатынасуды прокси-сервер арқылы жүзеге асыру көзделетін болса, онда iOS MDM веб-қызметі орнатылған құрылғыда келесі әрекеттерді орындау қажет:

1. Тізімдемеге келесі жолдарды жазу:

   - 32 разрядты операциялық жүйе үшін:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

   - 64 разрядты операциялық жүйе үшін:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Proxy Host Name>"
"ApnProxyPort"="<Proxy Port>"
"ApnProxyLogin"="<Proxy Login>"
"ApnProxyPwd"="<Proxy Password>"
```

2. Перезапустить веб-службу iOS MDM.

Ұялы құрылғыға жалпы сертификат беру және орнату

Пайдаланушыға жалпы сертификат шығару үшін:

1. Консоль ағашында **Пайдаланушы есептік жазбалары** қалтасында пайдаланушы есептік жазбасын таңдаңыз.
2. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Сертификатты орнату** тармағын таңдаңыз.

Сертификаттарды орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысы нәтижесінде, сертификат жасалып, пайдаланушы сертификаттары тізіміне қосылады.

Пайдаланушы жазылған сертификатты iOS MDM профилі бар орнату пакетімен бірге жүктейді.

Ұялы құрылғыны iOS MDM серверіне қосқаннан кейін, пайдаланушы құрылғысында iOS MDM профилінің параметрлері қолданылады. Әкімші қосылған құрылғыны басқара алады.

iOS MDM серверіне қосылған пайдаланушының ұялы құрылғысы консоль ағашының **Ұялы құрылғыларды басқару** қалтасына салынған **Ұялы құрылғылар қалтасында** көрсетіледі.

KES құрылғысын басқарылатын құрылғылар тізіміне қосу

Пайдаланушының KES құрылғысын Google Play™ дүкеніне сілтеменің көмегімен басқарылатын құрылғылар тізіміне қосу үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын таңдаңыз.

   Әдепкі бойынша, **Пайдаланушылардың есептік жазбалары** қалтасы **Кеңейтілген** қалтасына салынған.

2. Ұялы құрылғысын басқарылатын құрылғылар тізіміне қосқыңыз келетін пайдаланушының есептік жазбасын таңдаңыз.

3. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Ұялы құрылғыны қосу** тармағын таңдаңыз.

   Жаңа ұялы құрылғыны қосу шебері іске қосылды. **Сертификат көзі** шебері терезесінде, Басқару сервері ұялы құрылғыны идентификациялайтын жалпы сертификатты жасау тәсілін көрсету керек. Сіз жалпы сертификатты келесі екі тәсілдің бірімен белгілей аласыз:

   - Басқару серверінің құралдарымен жалпы сертификатты автоматты түрде жасау және құрылғыға сертификатты жеткізу;
   - жалпы сертификат файлын көрсету.

4. **Құрылғы түрі** шебері терезесінде **Google Play дүкеніне сілтеме** нұсқасын таңдаңыз.

5. **Пайдаланушыға хабарлау әдісі** шебері терезесінде ұялы құрылғы пайдаланушысын сертификаттың жасалғаны туралы хабарландыру параметрлерін конфигурациялаңыз (SMS-хабар, электрондық пошта арқылы немесе ақпарат шебердің жұмысы аяқталғаннан кейін көрсетіледі).

6. "Сертификаттар туралы ақпарат" шебері терезесінде шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Kaspersky Endpoint Security for Android шебердің жұмысы нәтижесінде, пайдаланушының құрылғысына Google Play дүкенінен жүктеп алу үшін сілтеме және QR коды жіберілетін болады. Пайдаланушы сілтемені пайдалану немесе QR кодын сканерлеу арқылы Google Play-ге өтеді. Содан кейін құрылғының операциялық жүйесі пайдаланушыдан Kaspersky Endpoint Security for Android орнатылымын қабылдауды сұрайды. Kaspersky Endpoint Security for Android қолданбасын жүктеп алып, орнатқаннан кейін, ұялы құрылғы Басқару серверіне қосылып, жалпы сертификатты жүктеп алады. Сертификатты ұялы құрылғыға орнатқаннан кейін, бұл құрылғы консоль шежіресінің **Мобильді құрылғыларды басқару** қалтасына салынған **Ұялы құрылғылар** қалтасында көрсетілетін болады.

> Kaspersky Endpoint Security for Android қолданбасы құрылғыға әлдеқашан орнатылған болса, пайдаланушы әкімшіден Басқару серверіне қосылу параметрлерін алып, оларды өз бетінше енгізуі керек. Қосылым параметрлерін конфигурациялағаннан кейін, ұялы құрылғы Басқару серверіне қосылады. Әкімші құрылғыға жалпы сертификатты жазып береді және пайдаланушыға сертификатты жүктеп алу үшін пайдаланушы аты мен құпиясөзі бар электрондық пошта хабарын немесе SMS-хабарды жібереді. Пайдаланушы жалпы сертификатты алып, орнатады. Сертификатты ұялы құрылғыға орнатқаннан кейін, бұл құрылғы консоль шежіресінің **Мобильді құрылғыларды басқару** қалтасына салынған **Ұялы құрылғылар** қалтасында көрсетілетін болады. Бұл жағдайда, Kaspersky Endpoint Security for Android қолданбасын қайтадан жүктеп алу және орнату орындалмайды.

KES құрылғыларын Басқару серверіне қосу

Құрылғыларды Басқару серверіне қосу тәсіліне байланысты, KES құрылғылары үшін Kaspersky Device Management for iOS орналастырудың екі схемасы бар:

- Басқару серверіне құрылғыларды тікелей қосу арқылы орналастыру схемасы;
- Kerberos Constrained Delegation қолдайтын кері прокси-серверді қолданатын орналастыру диаграммасы.

Құрылғыларды Басқару серверіне тікелей қосу

KES құрылғылары Басқару серверінің 13292 портына тікелей қосыла алады.

Түпнұсқалық растама тәсіліне байланысты, KES құрылғыларын Басқару серверіне қосудың екі нұсқасы бар:

- Пайдаланушы сертификатын қолдану арқылы құрылғыларды қосу
- Пайдалану сертификатынсыз құрылғыларды қосу

Пайдаланушы сертификатын қолдану арқылы құрылғыны қосу

Пайдаланушы сертификатын қолдану арқылы құрылғыны қосу кезінде, осы құрылғы Басқару серверінің құралдарымен тиісті сертификат тағайындалған пайдаланушының есептік жазбасына байланады.

Бұл жағдайда, екі жақты SSL түпнұсқалық растамасы (mutual authentication) қолданылады. Басқару сервері де, құрылғы да сертификаттардың көмегімен түпнұсқалық растамадан өткізіледі.

Пайдалану сертификатынсыз құрылғыны қосу

Пайдаланушы сертификатынсыз құрылғыны қосу кезінде, ол Басқару серверіндегі ешбір пайдаланушы есептік жазбасына байланбайды. Бірақ құрылғы кез келген сертификатты алған кезде, бұл құрылғы Басқару серверінің құралдарымен тиісті сертификат тағайындалған пайдаланушыға байланады.

Құрылғыны Басқару серверіне қосу кезінде бір жақты SSL түпнұсқалық растамасы (one-way SSL authentication) қолданылып, Басқару сервері сертификаттың көмегімен түпнұсқалық растамадан өтеді. Құрылғы пайдаланушы сертификатын алған кезде, түпнұсқалық растама түрі екі жақты SSL түпнұсқалық растамасына (2-way SSL authentication, mutual authentication) өзгертіледі.

Kerberos (KCD) мәжбүрлеп табыстау арқылы KES құрылғыларын Серверге қосу схемасы

KES құрылғыларын Kerberos Constrained Delegation (KCD) көмегімен Басқару серверіне қосу схемасы мыналарды қамтиды:

- KCD қолдайтын кері прокси-сервермен интеграция;
- ұялы құрылғылардың түпнұсқалық растамасы үшін Kerberos Constrained Delegation (бұдан әрі KCD) мәжбүрлеп табыстауын пайдалану;
- пайдаланушы сертификаттарын пайдалану үшін жалпыға ортақ кілттер инфрақұрылымымен (Public Key Infrastructure, бұдан әрі PKI) біріктіру.

Осы қосылым схемасын пайдалану кезінде мыналарды ескеру қажет:

- KES құрылғыларын кері прокси-серверге қосылым түрі "two-way SSL authentication" болуы тиіс, яғни құрылғы кері прокси-серверге өзінің пайдаланушы сертификаты арқылы қосылуы керек. Бұл үшін құрылғыда орнатылған Kaspersky Endpoint Security for Android орнату пакетіне пайдаланушы сертификатын кіріктіру қажет. Бұл KES пакетін осы құрылғы (пайдаланушы) үшін арнайы Басқару сервері жасауы керек.
- Мобильді протокол үшін әдепкі бойынша серверлік сертификаттың орнына арнайы (кастомизацияланған) сертификат көрсетілуі керек:
  1. Басқару сервері сипаттары терезесінде, **Параметрлер** бөлімінде **Ұялы құрылғыларға арналған портты ашу** жалаушасын қою және ашылмалы тізімнен **Сертификат қосу** тармағын таңдау.
  2. Ашылған терезеде, Басқару серверінде мобильді протоколға қатынасу нүктесін жариялау кезінде кері прокси-серверде берілген дәл сол сертификатты көрсетіңіз.
- KES құрылғылары үшін пайдаланушы сертификаттарын домендік Certificate Authority (CA) шығаруы керек. Доменде бірнеше түбірлік CA болса, онда пайдаланушы сертификаттары кері прокси-серверге арналған жарияланымда жазылған CA тарапынан шығарылуы тиіс.

Пайдаланушы сертификатының жоғарыда айтылған талапқа сәйкестігі бірнеше тәсілмен қамтамасыз етілуі мүмкін:

- Орнату пакеттерін жасау шеберінде және сертификаттарды орнату шеберінде арнайы пайдаланушы сертификатын көрсету.
- Басқару серверін домендік PKI инфрақұрылымымен біріктіру және сертификаттарды шығару ережелерінде тиісті параметрді конфигурациялау:

  1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Сертификаттар** салынған қалтасын таңдаңыз.
  2. **Сертификаттар** қалтасының жұмыс аймағында, **Сертификат беру ережелерін конфигурациялау** түймесі арқылы **Сертификаттарды шығару ережелері** терезесін ашыңыз.
  3. **PKI жүйесімен интеграциялау** бөлімінде жалпыға ортақ кілт инфрақұрылымымен біріктіруді конфигурациялаңыз.
  4. **Ұялы құрылғы сертификаттарын шығару** бөлімінде сертификаттар көзін көрсетіңіз.

Келесі болжамдармен KCD шектеулі табыстау конфигурациясы мысалын қарастырайық:

- Басқару серверінде мобильді протоколға қатынасу нүктесі 13292-портта көтерілген;
- кері прокси-серверден құрылғы атауы – firewall.mydom.local;
- Басқару сервері бар құрылғының атауы – ksc.mydom.local;
- Мобильді протоколға қатынасу нүктесін сырты жариялау атауы – kes4mob.mydom.global.

Басқару сервері үшін домендік есептік жазба

Басқару сервері қызметі жұмыс істейтін домендік есептік жазбаны (мысалы, KSCMobileSrvcUsr) жасау қажет. Басқару сервері қызметі үшін есептік жазбаны, Басқару серверін орнату кезінде немесе klsrvswch утилитасын пайдалану арқылы көрсетуге болады. klsrvswch утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Домендік есептік жазбаны келесі себептерге байланысты көрсету қажет:

- KES құрылғыларын басқару бойынша функционалдылық Басқару серверінің ажырамас бөлігі болып табылады.
- Мәжбүрлеп табыстау (KCD) дұрыс жұмыс істеуі үшін Басқару сервері болып табылатын қабылдаушы тарап домендік есептік жазбада жұмыс істеуі керек.

http/kes4mob.mydom.local үшін Service Principal Name

KSCMobileSrvcUsr есептік жазбасы бар доменде, Басқару сервері бар құрылғының 13292-портында мобильді протокол сервисінің жариялаңымы үшін Service Principal Name (SPN) жазу керек. Басқару сервері бар kes4mob.mydom.local құрылғысы үшін бұл келесідей көрінетін болады:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Кері прокси-сервері бар құрылғылардың домен сипаттарын конфигурациялау (firewall.mydom.local)

Трафикті табыстау үшін кері прокси-сервері (firewall.mydom.local) бар құрылғыны SPN (http/kes4mob.mydom.local:13292) бойынша анықталған қызметке сеніп тапсыру қажет.

Кері прокси-сервері бар құрылғыны SPN (http/kes4mob.mydom.local:13292) бойынша анықталған қызметке сеніп тапсыру үшін, әкімші келесі әрекеттерді орындауы тиіс:

1. Microsoft Management Console "Active Directory Users and Computers" жабдықтарында кері прокси-сервері (firewall.mydom.local) орнатылған құрылғыны таңдаңыз.

2. **Delegation** қойыншасындағы құрылғының сипаттарында **Trust this computer for delegation to specified service only** қосқышы үшін **Use any authentication protocol** нұсқасын таңдау.

3. **Services to which this account can present delegated credentials** тізіміне SPN http/kes4mob.mydom.local:13292.

Жарияланым үшін ерекше (кастомизацияланған) сертификат (kes4mob.mydom.global)

Басқару серверінің мобильді протоколын жариялау үшін FQDN kes4mob.mydom.global мекенжайына арнайы (кастомизацияланған) сертификат шығару және оны әдепкі бойынша серверлік сертификаттың орнына Басқару консоліндегі Басқару сервері мобильді протоколының параметрлерінде көрсету керек. Бұл үшін, Басқару сервері сипаттары терезесінде, **Параметрлер** бөлімінде **Ұялы құрылғыларға арналған портты ашу** жалаушасын қою және ашылмалы тізімнен **Сертификат қосу** тармағын таңдау керек.

Серверлік сертификаты бар контейнерде (p12 немесе pfx кеңейтімі бар файл) түбірлік сертификаттар тізбегі (жария бөліктер) болуы керек екенін де ескеру қажет.

Кері прокси-серверге жариялауды баптау

Кері прокси-серверде ұялы құрылғы тарапынан kes4mob.mydom.global атты 13292-портқа баратын трафик үшін, FQDN kes4mob.mydom.global атауына арнап шығарылған серверлік сертификатты қолдану арқылы SPN http/kes4mob.mydom.local:13292 мекенжайына KCD конфигурациялау керек. Жарияланымда да, жарияланатын қатынасу нүктесінде де (Басқару серверінің 13292-порты) бірдей серверлік сертификат болуы керек екенін ескеру қажет.

Firebase Cloud Messaging қолдану

Kaspersky Security Center-де Android операциялық жүйесі басқаратын KES құрылғыларына пәрмендерді уақтылы жеткізу үшін push-нотификациялар механизмі пайдаланылады. KES құрылғылары мен Басқару сервері арасындағы push-нотификациялар Firebase Cloud Messaging (бұдан әрі – FCM) сервисінің көмегімен жүзеге асырылады. Kaspersky Security Center Басқару консолінде KES құрылғыларын осы сервиске қосу үшін Cloud Messaging сервисінің параметрлерін көрсете аласыз.

Firebase Cloud Messaging параметрлерін алу үшін Google есептік жазбаңыз болуы керек.

FCM қолдануды қосу үшін:

1. Басқару консолінен **Мобильді құрылғыларды басқару** түйіні мен **Ұялы құрылғылар** торабын таңдаңыз.

2. **Ұялы құрылғылар** қалтасының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.

3. Қалта сипаттары терезесінен **Firebase Cloud Messaging параметрлері** бөлімін таңдаңыз.

4. **Firebase жобасының нөмірі** өрісінде Sender ID FCM енгізіңіз.

5. **Жеке кілт файлы (JSON пішімінде)** өрісінде жеке кілт файлын таңдаңыз.

   Басқару серверімен келесі жолы синхрондау кезінде, Android операциялық жүйесі басқаратын KES құрылғылары Firebase Cloud Messaging қызметіне қосылатын болады.

Firebase Cloud Messaging параметрлерін **Параметрлер бастапқы мәнге келтірілуде** түймесі арқылы өзгерте аласыз.

Басқа Firebase жобасына ауысқанда, FCM жұмысы 10 минуттан кейін жалғасады.

FCM сервисі келесі мекенжайлар ауқымында жұмыс істейді:

- KES құрылғылары тарапынан 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) порттарына келесі мекенжайлардан қатынасу мүмкіндігі қажет:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - немесе "Google ASN 15169" тізіміндегі барлық IP мекенжайларына
- Басқару сервері тарапынан 443-портқа (HTTPS) келесі мекенжайлардан қатынасу қажет:
  - fcm.googleapis.com
  - немесе "Google ASN 15169" тізіміндегі барлық IP мекенжайларына

Басқару консолінде Басқару серверінің сипаттарында прокси-сервердің параметрлері (**Қосымша** / **Интернет желісіне қатынасу параметрлері**) көрсетілген болса, олар FCM-мен өзара әрекеттесу үшін пайдаланылатын болады.

FCM орнату: Sender ID мен жабық кілт файлын алу

FCM конфигурациялау үшін:

1. Google порталында тіркелу.

2. Firebase консоліне өтіңіз.

3. Келесі әрекеттердің бірін орындаңыз:

   - Жобаны жасау үшін **Жоба жасау** түймесін басып, экрандағы нұсқауларды орындаңыз.
   - Бар жобаны ашыңыз.

4. Тегершік белгішесін басып, **Жоба параметрлері** тармағын таңдаңыз.

   Жоба параметрлері терезесі ашылады.

5. **Cloud Messaging** қойындысын таңдаңыз.

6. **Firebase Cloud Messaging API (V1)** бөліміндегі **Sender ID** өрісінен Sender ID көшіріп алыңыз.

7. **Қызметтің есептік жазбалары** қойындысын таңдап, **Жаңа жеке кілтті жасау** түймесін басыңыз.

8. Ашылған терезеде жеке кілт файлын жасау және жүктеп салу үшін **Кілтті жасау** түймесін басыңыз.

Firebase Cloud Messaging конфигурацияланған.

Жалпыға ортақ кілттер инфрақұрылымымен біріктіру

Жалпыға ортақ кілттер инфрақұрылымымен (Public Key Infrastructure, бұдан әрі PKI) біріктіру, ең алдымен Басқару серверінің домендік пайдаланушы сертификаттарын шығаруын жеңілдетуге арналған.

Әкімші Басқару консолінде пайдаланушыға домендік сертификат тағайындай алады. Мұны келесі тәсілдердің бірімен жасауға болады:

- пайдаланушыға сертификаттарды орнату шеберіндегі файлдан арнайы (кастомизацияланған) сертификат тағайындау;

- PKI-мен біріктіруді жүзеге асырыңыз және PKI инфрақұрылымын сертификаттардың белгілі бір түріне немесе сертификаттардың барлық түрлеріне арналған сертификат көзі етіп тағайындаңыз.

PKI-мен біріктіру параметрлері **Ашық кілттердің инфрақұрылымымен интеграциялау** сілтемесінен өткен кезде **Мобильді құрылғыларды басқару** / **Сертификаттар** қалтасының жұмыс аймағында қолжетімді.

Пайдаланушылардың домендік сертификаттарын шығару үшін PKI-мен біріктірудің жалпы қағидаты

Басқару консолінде, **Мобильді құрылғыларды басқару** / **Сертификаттар** қалтасының жұмыс аймағындағы **Ашық кілттердің инфрақұрылымымен интеграциялау** сілтемесі арқылы, домендік CA арқылы домендік пайдаланушы сертификаттарын шығару үшін Басқару сервері тарапынан қолданылатын домендік есептік жазбаны (бұдан әрі – PKI-мен біріктіру орындалатын есептік жазба) белгілеу керек.

Назар аударыңыз:

- PKI-мен біріктіру параметрлерінде сертификаттардың барлық түрлері үшін әдепкі бойынша үлгіні көрсету мүмкіндігі бар. Бұл арада, сертификаттарды шығару ережелерінде (ережелер **Мобильді құрылғыларды басқару** / **Сертификаттар** қалтасының жұмыс аймағында, **Сертификат беру ережелерін конфигурациялау** түймесі арқылы қолжетімді) әрбір сертификат түрі үшін бөлек үлгі жасау мүмкіндігі бар.

- Басқару сервері орнатылған құрылғыда PKI-мен біріктіру жүргізілетін есептік жазбаның сертификаттар қоймасында Enrollment Agent (EA) мамандандырылған сертификаты орнатылуы керек. Enrollment Agent (EA) сертификатын домендік CA (Certificate Authority) әкімшісі шығарады.

PKI-мен біріктіру жүргізілетін есептік жазба келесі критерийлерге сәйкес келуі керек:

- Домен пайдаланушысы болып табылады.

- Бұл PKI-мен біріктіру жүзеге асырылатын орнатылған Басқару сервері бар құрылғының жергілікті әкімшісі.

- *Қызмет ретінде жүйеге кіру* құқығы бар.

- Бұл есептік жазбаның астында тұрақты пайдаланушы профилін жасау үшін Басқару сервері орнатылған құрылғыны кем дегенде бір рет іске қосу қажет.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (бұдан әрі Веб-сервер) – Kaspersky Security Center құрамдасы. Веб-сервер жеке орнату пакеттерін, ұялы құрылғыларға арналған жеке орнату пакеттерін, iOS MDM профильдерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды жариялауға арналған.

Құрылған iOS MDM профильдері және орнату пакеттері Веб-серверде автоматты түрде жарияланады және бірінші рет жүктегеннен кейін жойылады. Әкімші қалыптастырылған сілтемені пайдаланушыға кез келген ыңғайлы тәсілмен, мысалы, электрондық пошта арқылы жібере алады.

Алынған сілтеме арқылы, пайдаланушы ұялы құрылғыға арналған ақпаратты жүктей алады.

Веб-серверді конфигурациялау

Басқару консолі Веб-сервері сипаттарында Веб-серверді дәл конфигурациялау үшін HTTP (8060) және HTTPS (8061) протоколдарының порттарын ауыстыруға болады. Сондай-ақ, порттарды ауыстырудан бөлек, HTTPS протоколы үшін серверлік сертификатты ауыстыруға және HTTP протоколы үшін веб-сервер FQDN атауын ауыстыруға болады.

Kaspersky Security Center орнату

Бұл бөлімде Kaspersky Security Center құрамдастарын орнату тәсілі сипатталған. Бағдарламаны тек бір құрылғыға жергілікті түрде орнатқыңыз келсе, орнатудың екі нұсқасы қолжетімді:

- **Стандартты**. Kaspersky Security Center бағдарламасымен танысқыңыз келсе, мысалы, оның жұмысын ұйымыңыздың желісінің шағын бөлігінде сынағыңыз келсе, осы нұсқа ұсынылады. Стандартты орнату кезінде сіз тек дерекқор параметрлерін конфигурациялайсыз. Сондай-ақ, сіз тек Kaspersky бағдарламалары үшін әдепкі бойынша орнатылған басқару плагиндерінің жиынтығын ғана орната аласыз. Kaspersky Security Center бағдарламасымен жұмыс істеп көрсеңіз және стандартты орнатудан кейін сізге қажетті барлық параметрлерді қалай конфигурациялау керектігін білсеңіз, стандартты орнатуды пайдалана аласыз.

- **Таңдаулы**. Kaspersky Security Center параметрлерін, мысалы, ортақ қатынасы бар қалтаға апаратын жолды, есептік жазбаларды және Басқару серверіне қосылу порттары және дерекқор параметрлерін конфигурациялауды жоспарласаңыз, онда осы нұсқа ұсынылады. Таңдаулы орнату, Kaspersky бағдарламаларын басқару плагиндерінің қайсысы орнатылатынын көрсетуге мүмкіндік береді. Қажет болса, сіз таңдаулы орнатуды тыныш режимде іске қоса аласыз.

Желіде кем дегенде бір Басқару сервері орнатылған болса, желінің басқа құрылғыларындағы Серверлерді күштеп орнату әдісімен қашықтан орнату тапсырмасы арқылы орнатуға болады. Бағдарламаны қашықтан орнату тапсырмасын жасау кезінде Басқару серверінің орнату пакетін пайдалану қажет: ksc_<нұсқа_нөмірі>.<жинақ нөмірі>_full_<локализация тілі>.exe.

Kaspersky Security Center бағдарламасының барлық функцияларының жұмыс істеуіне қажетті барлық құрамдастарды орнатқыңыз келсе немесе осы құрамдастардың қолданыстағы нұсқаларын жаңартқыңыз келсе, осы пакетті қолданыңыз.

Ақауларға төзімді Kaspersky Security Center кластерін орналастырғыңыз келсе, Kaspersky Security Center бағдарламасын кластердің барлық түйіндеріне орнатуыңыз керек.

Орнатуға дайындық

Орнатуды бастамас бұрын келесі қадамдарды орындаңыз.

- **Жабдыққа және бағдарламалық жасақтамаға қойылатын талаптарды тексеру**

  Құрылғының аппараттық және бағдарламалық жасақтамасы Басқару сервері мен Басқару консоліне қойылатын талаптарға сай келетініне көз жеткізіңіз.

- **Дерекқорды басқару жүйесін (ДҚБЖ) таңдау және орнату**

  Kaspersky Security Center өз ақпаратын ДҚБЖ басқаратын дерекқорында сақтайды. Kaspersky Security Center орнатпас бұрын желіде ДҚБЖ орнатыңыз (ДҚБЖ таңдау туралы қосымша ақпарат алыңыз). Егер сіз PostgreSQL немесе Postgres Pro ДҚБЖ орнатуды шешсеңіз, суперпайдаланушының құпиясөзін көрсетіңіз. Егер құпиясөз көрсетілмесе, Басқару сервері дерекқорға қосылмауы мүмкін.

  Басқару серверін домен контроллеріне емес, бөлектенген серверге орнату ұсынылады. Тек оқуға арналған домен контроллері (RODC) рөлін атқаратын серверге Kaspersky Security Center орнатсаңыз, Microsoft SQL Server (SQL Express) жергілікті түрде орнатылмауы керек (дәл сол құрылғыда). Бұл жағдайда, Microsoft SQL Server (SQL Express) серверін қашықтан (басқа құрылғыға) орнату немесе ДҚБЖ жүйесін жергілікті түрде орнату қажет болса – MySQL, MariaDB не PostgreSQL пайдалану ұсынылады.

- **Басқару сервері, Желілік агент және Басқару консолі үшін қалталарды дайындау**

  Тіркелім есебі өшірілген қалталарға Басқару серверін, Желілік агент пен Басқару консолін орнату керек. Сондай-ақ, Басқару серверінің ортақ қатынасы бар қалтасы және Kaspersky Security Center жасырын қалтасы үшін тіркелім есебін өшіру қажет (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Желілік агенттің ескі нұсқасын жойыңыз**

  Басқару сервері құрамдасымен бірге құрылғыға Желілік агенттің серверлік нұсқасы орнатылады. Оны Желілік агенттің әдеттегі нұсқасымен бірге орнату мүмкін емес. Егер сіздің құрылғыңызда Желілік агенттің серверлік нұсқасы орнатылған болса, оны жойып, Басқару серверін орнатуды қайта іске қосу қажет. Желілік агент нұсқасы туралы толық ақпаратты Kaspersky Security Center орнатқаннан кейін жүйедегі өзгерістер бөлімінен қараңыз.

- **Есептік жазбаларды тексеру**

  Kaspersky Security Center орнату үшін орнату жүзеге асырылатын құрылғыда жергілікті әкімші құқықтары болуы қажет.

  Kaspersky Security Center бағдарламасы қызметтің басқарылатын есептік жазбаларын және қызметтің топтық басқарылатын есептік жазбаларын қолдайды. Егер бұл есептік жазба түрлері сіздің доменіңізде қолданылса және сіз олардың біреуін Басқару сервері қызметі үшін есептік жазба ретінде көрсеткіңіз келсе, алдымен есептік жазбаны Басқару серверін орнатқыңыз келетін құрылғыға орнатыңыз. Жергілікті құрылғыда қызметтердің басқарылатын есептік жазбаларын орнату туралы қосымша ақпаратты Microsoft ресми құжаттамасынан қараңыз.

ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар

Басқару серверін орнату және онымен жұмыс істеу үшін, сізге Басқару серверін орнату бағдарламасын (бұдан әрі "инсталлятор" деп те аталады) іске қосатын Windows есептік жазбасы, Басқару сервері қызметін іске қосатын Windows есептік жазбасы және ДҚБЖ-не қатынасу үшін ДҚБЖ ішкі есептік жазбасы керек болады. Есептік жазбаларды жасауға немесе қолданыстағыларды қолдануға болады. Осы есептік жазбалардың барлығы белгілі бір құқықтарды талап етеді. Қажетті есептік жазбалар жиынтығы және олардың құқықтары келесі өлшемшарттарға байланысты:

- ДҚБЖ түрі:
  - Microsoft SQL Server (Windows түпнұсқалық растамасымен немесе SQL Server түпнұсқалық растамасымен)
  - MySQL немесе MariaDB
  - PostgreSQL немесе Postgres Pro
- ДҚБЖ орналасуы:
  - **Жергілікті ДҚБЖ**. *Жергілікті ДҚБЖ* — басқару серверімен бір құрылғыда орнатылған ДҚБЖ.
  - **қашықтағы ДҚБЖ**. *Қашықтағы ДҚБЖ* деп, басқа құрылғыға орнатылған ДҚБЖ аталады.
- Басқару сервері дерекқорын құру тәсілі:
  - **Автоматты түрде**. Басқару серверін орнатқан кезде инсталлятор көмегімен Басқару серверінің дерекқорын (бұдан әрі Сервер дерекқоры деп те аталады) автоматты түрде жасауға болады.
  - **Қолмен**. Бос дерекқорды құру үшін үшінші тарап бағдарламасын (мысалы, SQL Server Management Studio) немесе скриптті пайдалануға болады. Содан соң, Басқару серверін орнату кезінде осы дерекқорды Сервердің дерекқоры ретінде көрсете аласыз.

Есептік жазбаларға құқықтар мен рұқсаттар беру кезінде ең аз артықшылықтар қағидатын ұстаныңыз. Бұл, берілген құқықтар тек қажетті әрекеттерді орындау үшін жеткілікті екенін білдіреді.

Төмендегі кестелерде, Басқару серверін орнатпас бұрын және іске қоспас бұрын есептік жазбаларға ұсынылуы тиісті жүйелік құқықтар және ДҚБЖ-не арналған құқықтар туралы ақпарат бар.

Windows түпнұсқалық растамасы бар Microsoft SQL Server

Егер сіз SQL Server серверін ДҚБЖ ретінде таңдасаңыз, SQL Server серверіне қатынасу үшін Windows түпнұсқалық растамасын пайдалануға болады. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасына және Басқару сервері қызметін іске қосу үшін пайдаланылатын Windows есептік жазбасына жүйелік құқықтарды конфигурациялаңыз. SQL Server серверінде осы Windows есептік жазбалары үшін есептік жазбалар жасаңыз. Сервер дерекқорын құру әдісіне байланысты төмендегі кестеде сипатталғандай осы есептік жазбаларға қажетті SQL Server құқықтарын ұсыныңыз. Есептік құқықтарын теңшеу туралы толығырақ SQL Server жүйесімен жұмыс істеу үшін есептік жазбаларды теңшеу (Windows түпнұсқалық растамасы) бөлімін қараңыз.

ДҚБЖ: Windows түпнұсқалық растамасы бар Microsoft SQL Server (соның ішінде Express Edition)

	Дерекқорды автоматты түрде жасау (орнату бағдарламасы арқылы)	Дерекқорды қолмен жасау (әкімші тарапынан)
Инсталлятор жұмыс істейтін есептік жазба	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.
Инсталлятор жұмыс істейтін есептік жазба құқықтары	• Жүйелік құқықтар: жергілікті әкімші құқықтары. • SQL Server құқықтары: • Сервер деңгейінің рөлі: sysadmin.	• Жүйелік құқықтар: жергілікті әкімші құқықтары. • SQL Server құқықтары: • Сервер деңгейінің рөлі: public. • Сервер дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner, public. • Сервер дерекқорының әдепкі бойынша схемасы: dbo.
Басқару сервері қызметінің есептік жазбасы	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба.	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба (бұл жағдайда KL-AK-* есептік жазбасын жасау ұсынылмайды).
Басқару сервері қызметі есептік жазбасының құқықтары	• Жүйелік құқықтар: инсталлятор берген қажетті құқықтар. • SQL Server құқықтары: инсталлятор берген қажетті құқықтар.	• Жүйелік құқықтар: инсталлятор берген қажетті құқықтар. • SQL Server құқықтары: • Сервер деңгейінің рөлі: public. • Сервер дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner, public. • Сервер дерекқорының әдепкі бойынша схемасы: dbo.

SQL Server түпнұсқалық растамасы бар Microsoft SQL Server

Егер сіз SQL Server серверін ДҚБЖ ретінде таңдасаңыз, SQL Server серверіне қосылу үшін SQL Server түпнұсқалық растамасын пайдалана аласыз. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасына және Басқару серверімен жұмыс істеу үшін пайдаланылатын Windows есептік жазбасына жүйелік құқықтарды конфигурациялаңыз. SQL Server серверінде, оны түпнұсқалық растама үшін пайдалану мақсатында құпиясөзі бар есептік жазба жасаңыз. Содан кейін, осы SQL Server есептік жазбасына төмендегі кестеде көрсетілген қажетті құқықтарды беріңіз. Есептік құқықтарын теңшеу туралы толығырақ SQL Server жүйесімен жұмыс істеу үшін есептік жазбаларды теңшеу (SQL Server түпнұсқалық растамасы) бөлімін қараңыз.

ДҚБЖ: SQL Server түпнұсқалық растамасы бар Microsoft SQL Server (соның ішінде Express Edition)

	Дерекқорды автоматты түрде жасау (орнату бағдарламасы арқылы)	Дерекқорды қолмен жасау (әкімші тарапынан)
Инсталлятор жұмыс істейтін есептік жазба	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.

	Дерекқорды автоматты түрде жасау (орнату бағдарламасы арқылы)	Дерекқорды қолмен жасау (әкімші тарапынан)
Инсталлятор жұмыс істейтін есептік жазба құқықтары	Жүйелік құқықтар: жергілікті әкімші құқықтары.	Жүйелік құқықтар: жергілікті әкімші құқықтары.
Басқару сервері қызметінің есептік жазбасы	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба.	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows пайдаланушысы есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба.
Басқару сервері қызметі есептік жазбасының құқықтары	Жүйелік құқықтар: инсталлятор берген қажетті құқықтар.	Жүйелік құқықтар: инсталлятор берген қажетті құқықтар.
SQL Server түпнұсқалық растамасы үшін пайдаланылатын есептік жазба құқықтары	Дерекқор жасау және Басқару серверін орнату үшін қажет SQL Server құқықтары: • Сервер деңгейінің рөлі: public. • *master* дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner. • *master* дерекқорының әдепкі бойынша схемасы: dbo. • Рұқсаттар: • CONNECT ANY DATABASE • CONNECT SQL • CREATE ANY DATABASE • VIEW ANY DATABASE • VIEW SERVER STATE (**Always On** параметрі қосулы болса) Басқару сервермен жұмыс істеу үшін қажет SQL Server құқықтары: • Сервер деңгейінің рөлі: public. • Сервер дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner. • Сервер дерекқорының әдепкі бойынша схемасы: dbo. • Рұқсаттар: • CONNECT SQL • VIEW ANY DATABASE • VIEW SERVER STATE (**Always On** параметрі қосулы болса) • VIEW ANY DEFINITION	SQL Server құқықтары: • Сервер деңгейінің рөлі: public. • Сервер дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner. • Сервер дерекқорының әдепкі бойынша схемасы: dbo. • Рұқсаттар: • CONNECT SQL • VIEW ANY DATABASE • VIEW ANY DEFINITION

Басқару сервері деректерін қалпына келтіру үшін SQL Server құқықтарын конфигурациялау

Сақтық көшірмеден Басқару сервері деректерін қалпына келтіру үшін, Басқару сервері орнатылған Windows есептік жазбасымен klbackup утилитасын іске қосыңыз. klbackup утилитасын SQL Server серверінде іске қоспас бұрын, осы Windows есептік жазбасымен байланысты SQL Server серверіне кіру құқығын беріңіз. SQL Server құқықтары Басқару сервері нұсқасына байланысты өзгереді. Басқару серверінің 14.2 және одан жоғары нұсқасы үшін sysadmin серверлік рөлін немесе dbcreator серверлік рөлін тағайындауға болады.

Басқару сервері дерекқорын қалпына келтіруге арналған SQL Server құқықтары

Басқару серверінің 14.2 және одан жоғары нұсқасы	Басқару серверінің басқа да нұсқалары
• SQL Server құқықтары: • Сервер деңгейінің рөлі: dbcreator. • Рұқсаттар: • VIEW ANY DEFINITION klbackup утилитасын іске қосар алдында KLSRV_SKIP_ADJUSTING_DBMS_ACCESS сервері жалаушасын көрсетіңіз. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Содан кейін пәрмен жолында келесі пәрменді орындаңыз: `klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL және MariaDB

Егер сіз MySQL немесе MariaDB серверін ДҚБЖ ретінде таңдасаңыз, ДҚБЖ ішкі есептік жазбасын жасаңыз және осы есептік жазбаға төмендегі кестеде көрсетілген қажетті құқықтарды беріңіз. Басқару сервері қызметі және орнату бағдарламасы ДҚБЖ-не қатынасу үшін осы ДҚБЖ ішкі есептік жазбасын пайдаланады. Дерекқорды құру тәсілі қажетті құқықтар жиынтығына әсер етпейтінін ескеріңіз. Есептік жазба құқықтарын конфигурациялау туралы толығырақ MySQL және MariaDB серверлерімен жұмыс істеу үшін есептік жазбаларды конфигурациялау бөлімінен қараңыз.

ДҚБЖ: MySQL және MariaDB

	Дерекқорды автоматты түрде немесе қолмен жасау
Инсталлятор жұмыс істейтін есептік жазба	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.
Инсталлятор жұмыс істейтін есептік жазба құқықтары	Жүйелік құқықтар: жергілікті әкімші құқықтары.
Басқару сервері қызметінің есептік жазбасы	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба.
Басқару сервері қызметі есептік жазбасының құқықтары	Жүйелік құқықтар: инсталлятор берген қажетті құқықтар.
ДҚБЖ ішкі есептік жазбасы құқықтары	Артықшылықтар схемасы: • Басқару сервері дерекқоры: ALL (GRANT OPTION қоспағанда). • Жүйе схемалары (mysql және sys): SELECT, SHOW VIEW. • Сақталатын sys.table_exists процедурасы: EXECUTE (MariaDB 10.5 немесе одан бұрынғы нұсқасын ДҚБЖ ретінде пайдаланасаңыз, сізге EXECUTE құқығын берудің қажеті жоқ). Барлық схемаларға арналған жаһандық артықшылықтар: PROCESS, SUPER.

Деректерді ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу жолы туралы мәліметтерді Деректерді MySQL және MariaDB ДҚБЖ-лардағы ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу бөлімін қараңыз.

Басқару сервері деректерін қалпына келтіру құқықтарын конфигурациялау

ДҚБЖ ішкі есептік жазбасы үшін берген құқықтарыңыз сақтық көшірмеден Басқару сервері деректерін қалпына келтіруге жеткілікті. Қалпына келтіруді бастау үшін, Басқару сервері орнатылған Windows есептік жазбасымен klbackup утилитасын іске қосыңыз.

PostgreSQL немесе Postgres Pro

PostgreSQL немесе Postgres Pro жүйесін ДҚБЖ ретінде таңдасаңыз, *Postgres* пайдаланушысын (әдепкі бойынша Postgres рөлін) қолдана аласыз немесе ДҚБЖ-не қатынасу үшін Postgres рөлін (бұдан әрі рөл деп те аталады) жасай аласыз. Сервер дерекқорын жасау тәсіліне байланысты, төмендегі кестеде сипатталғандай рөлге қажетті құқықтарды беріңіз. Рөл құқықтарын теңшеу туралы толығырақ PostgreSQL немесе Postgres Pro жүйесімен жұмыс істеу үшін есептік жазбаларды теңшеу бөлімін қараңыз.

ДҚБЖ: PostgreSQL немесе Postgres Pro

	Дерекқорды автоматты түрде жасау		Дерекқорды қолмен жасау
Инсталлятор жұмыс істейтін есептік жазба	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.		• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: жергілікті әкімшінің есептік жазбасы немесе доменнің есептік жазбасы.
Инсталлятор жұмыс істейтін есептік жазба құқықтары	Жүйелік құқықтар: жергілікті әкімші құқықтары.		Жүйелік құқықтар: жергілікті әкімші құқықтары.
Басқару сервері қызметінің есептік жазбасы	• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба.		• Қашықтағы ДҚБЖ: ДҚБЖ орнатылған қашықтағы құрылғының домендік есептік жазбасы ғана. • Жергілікті ДҚБЖ: • Әкімші таңдаған Windows есептік жазбасы. • Орнату бағдарламасы автоматты түрде жасайтын KL-AK-* пішіміндегі есептік жазба.
Басқару сервері қызметі есептік жазбасының құқықтары	Жүйелік құқықтар: инсталлятор берген қажетті құқықтар.		Жүйелік құқықтар: инсталлятор берген қажетті құқықтар.
Postgres рөлі құқықтары	*Postgres* пайдаланушысына қосымша құқықтар қажет емес.	Жаңа рөлге арналған құқықтар: `CREATEDB`.	Жаңа рөл үшін: • Басқару сервері дерекқорына қатынасу құқықтары: `ALL`. • Жалпыға ортақ схемадағы барлық кестелерге қатынасу құқықтары: `ALL`. • Жалпыға ортақ схемадағы барлық бірізділіктерге қатынасу құқықтары: `ALL`.

Басқару сервері деректерін қалпына келтіру құқықтарын конфигурациялау

Сақтық көшірмеден Басқару сервері деректерін қалпына келтіру үшін, Басқару сервері орнатылған Windows есептік жазбасымен klbackup утилитасын іске қосыңыз. ДҚБЖ-ға қатынасу үшін пайдаланылатын Postgres рөлінде иеленушінің Басқару сервері дерекқорына қатысты құқықтары болуы керек екенін ескеріңіз.

SQL Server серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау (Windows түпнұсқалық растамасы)

Алдын ала талаптар

Есептік жазбаларға құқықтарды тағайындамас бұрын келесі әрекеттерді орындаңыз:

1. Жергілікті әкімші есептік жазбасымен кіргеніңізге көз жеткізіңіз.
2. SQL Server серверімен жұмыс істеуге арналған ортаны орнатыңыз.
3. Басқару сервері орнатылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.
4. Басқару сервері қызметі іске қосылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.
5. SQL Server серверіне Басқару серверін орнату бағдарламасын (бұдан әрі "инсталлятор" деп те аталады) іске қосу үшін қолданылатын Windows есептік жазбасы үшін есептік жазбаны жасаңыз. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын да жасаңыз.

SQL Server Management Studio бағдарламасын қолдансаңыз, онда кіру сипаттары терезесінің **Жалпы** бетінде **Windows түпнұсқалық растамасы** параметрін таңдаңыз.

> Басқару серверін және SQL серверін әртүрлі Windows домендерінде орналасқан құрылғыларға орнатқыңыз келсе, бұл домендерде Басқару серверінің дұрыс жұмысын, соның ішінде тапсырманы орындауды және саясатты орындауды қамтамасыз ету үшін екі жақты сенімді қарым-қатынастар болуы керек екенін ескеріңіз. Әртүрлі ДҚБЖ-мен жұмыс істеуге қажетті есептік жазбалар және есептік жазбалардың құқықтары туралы ақпаратты ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар бөлімінен қараңыз.

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын автоматты түрде жасау)

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. SQL Server серверінде sysadmin рөлін орнату бағдарламасын іске қосу үшін қолданылатын Windows есептік жазбасына арналған сервер деңгейінде тағайындаңыз.
2. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасымен жүйеге кіріңіз.
3. Басқару серверін орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
4. Басқару серверінің таңдаулы орнатылымын таңдаңыз.
5. Басқару сервері дерекқоры сақталатын ДҚБЖ ретіндегі Microsoft SQL Server тармағын таңдаңыз.

6. Басқару сервері мен SQL Server арасында Windows есептік жазбасының көмегімен қосылым орнату үшін Microsoft Windows аутентификация режимі тармағын таңдаңыз.

7. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

   Бұған дейін SQL Server есептік жазбасы жасалған Windows пайдаланушы есептік жазбасын таңдауға болады. Бұдан бөлек, орнату бағдарламасының көмегімен KL-AK-* пішімінде Windows есептік жазбасын автоматты түрде жасай аласыз. Бұл жағдайда, орнату бағдарламасы автоматты түрде сол есептік жазба үшін SQL Server есептік жазбасын жасайды. Есептік жазбаны таңдауға қарамастан, орнату бағдарламасы Басқару сервері қызметінің есептік жазбасына қажетті жүйелік құқықтар мен SQL Server құқықтарын тағайындайды.

Орнату аяқталғаннан кейін, Сервер дерекқоры жасалады және барлық қажетті жүйелік құқықтар мен SQL Server құқықтары Басқару сервері қызметінің есептік жазбасына тағайындалады. Басқару сервері жұмыс істеуге дайын.

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын қолмен жасау)

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. SQL Server серверінде бос дерекқор жасаңыз. Бұл дерекқор Басқару сервері дерекқоры ретінде пайдаланылады (бұдан әрі Сервер дерекқоры).

2. Windows есептік жазбалары үшін жасалған екі SQL Server есептік жазбасы үшін де сервер деңгейінің жалпыға қолжетімді рөлін көрсетіңіз және құрылған дерекқормен салыстыруды конфигурациялаңыз:

   - Сервер деңгейінің рөлі: public.
   - Дерекқорлар мүшелігі рөлі: db_owner, public.
   - Әдепкі бойынша схема: dbo.

3. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасымен жүйеге кіріңіз.

4. Басқару серверін орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

5. Басқару серверінің таңдаулы орнатылымын таңдаңыз.

6. Басқару сервері дерекқоры сақталатын ДҚБЖ ретіндегі Microsoft SQL Server тармағын таңдаңыз.

7. Құрылған дерекқордың атауын Басқару сервері дерекқорының атауы ретінде көрсетіңіз.

8. Басқару сервері мен SQL Server арасында Windows есептік жазбасының көмегімен қосылым орнату үшін Microsoft Windows аутентификация режимі тармағын таңдаңыз.

9. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

   Сіз бұған дейін SQL Server кіру есептік жазбасын жасаған және кіру құқығын конфигурациялаған Windows пайдаланушы есептік жазбасын таңдай аласыз.

Windows есептік жазбасын KL-AK-* пішімінде автоматты түрде жасау ұсынылмайды. Бұл жағдайда, орнату бағдарламасы сіз SQL Server есептік жазбасын жасамаған немесе конфигурацияламаған Windows есептік жазбасын жасайды. Басқару сервері бұл есептік жазбаны Басқару сервері қызметін іске қосу үшін пайдалана алмайды. Windows KL-AK-* есептік жазбасын жасау қажет болса, орнатқаннан кейін Басқару консолін іске қоспаңыз. Мұның орнына, келесі әрекеттерді орындаңыз:

1. kladminserver қызметін тоқтатыңыз.
2. SQL Server серверінде, жасалған Windows KL-AK-* есептік жазбасы үшін SQL Server есептік жазбасын жасаңыз.
3. Осы SQL Server есептік жазбасына құқықтар беріңіз және жасалған дерекқормен салыстыруды конфигурациялаңыз:
   - Сервер деңгейінің рөлі: public.
   - Дерекқорлар мүшелігі рөлі: db_owner, public.
   - Әдепкі бойынша схема: dbo.
4. kladminserver қызметін қайта іске қосыңыз, содан кейін Басқару консолін іске қосыңыз.

Орнату аяқталғаннан кейін, Басқару сервері Сервердің деректерін сақтау үшін құрылған дерекқорды пайдаланады. Басқару сервері жұмыс істеуге дайын.

SQL Server серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау (SQL Server түпнұсқалық растамасы)

Алдын ала талаптар

Есептік жазбаларға құқықтарды тағайындамас бұрын келесі әрекеттерді орындаңыз:

1. Жергілікті әкімші есептік жазбасымен кіргеніңізге көз жеткізіңіз.
2. SQL Server серверімен жұмыс істеуге арналған ортаны орнатыңыз.
3. Басқару сервері орнатылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.
4. Басқару сервері қызметі іске қосылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.
5. SQL Server серверінде SQL Server түпнұсқалық растамасы режимін қосыңыз.

   Егер сіз SQL Server Management Studio бағдарламасын қолдансаңыз, **Қауіпсіздік** бетіндегі SQL Server сипаттары терезесінде **SQL Server және Windows түпнұсқалық растамасы режимі** параметрін таңдаңыз.

6. SQL Server серверінде құпиясөзі бар есептік жазба жасаңыз. Басқару серверін орнату бағдарламасы (орнату бағдарламасы) және Басқару сервері қызметі SQL Server серверіне қатынасу үшін осы SQL Server есептік жазбасын пайдаланады.

   SQL Server Management Studio бағдарламасын қолдансаңыз, онда кіру сипаттары терезесінің **Жалпы** бетінде **SQL сервері түпнұсқалық растамасы** параметрін таңдаңыз.

Басқару серверін және SQL серверін әртүрлі Windows домендерінде орналасқан құрылғыларға орнатқыңыз келсе, бұл домендерде Басқару серверінің дұрыс жұмысын, соның ішінде тапсырманы орындауды және саясатты орындауды қамтамасыз ету үшін екі жақты сенімді қарым-қатынастар болуы керек екенін ескеріңіз. Әртүрлі ДҚБЖ-мен жұмыс істеуге қажетті есептік жазбалар және есептік жазбалардың құқықтары туралы ақпаратты ДҚБЖ-мен жұмыс істеуге арналған есептік жазбалар бөлімінен қараңыз.

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын автоматты түрде жасау)

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. SQL Server серверінде SQL Server есептік жазбасын *master* дерекқорындағы әдепкі бойынша есептік жазбамен салыстырыңыз. *master* дерекқоры Басқару сервері дерекқорының үлгісі болып табылады (бұдан әрі Сервер дерекқоры). *master* дерекқоры, орнату бағдарламасы Сервер дерекқорын жасағанға дейін салыстыру үшін пайдаланылады SQL Server есептік жазбасына келесі құқықтар мен рұқсаттар беріңіз:

   - Сервер деңгейінің рөлі: public.
   - *master* дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner.
   - *master* дерекқорының әдепкі бойынша схемасы: dbo.
   - Рұқсаттар:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE

2. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасымен жүйеге кіріңіз.

3. Орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

4. Басқару серверінің таңдаулы орнатылымын таңдаңыз.

5. Басқару сервері дерекқоры сақталатын ДҚБЖ ретіндегі Microsoft SQL Server тармағын таңдаңыз.

6. Басқару сервері дерекқорының атауын көрсетіңіз.

7. Жасалған SQL Server есептік жазбасының көмегімен Басқару сервері мен SQL Server арасында қосылым орнату үшін SQL Server түпнұсқалық растамасы режимі тармағын таңдаңыз. Содан соң, SQL Server есептік жазбасы деректерін көрсетіңіз.

8. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

   Сіз бар Windows пайдаланушы есептік жазбасын таңдай аласыз немесе орнату бағдарламасын пайдаланып, KL-AK-* Windows есептік жазбасын жасай аласыз. Таңдалған есептік жазбаға қарамастан, орнату бағдарламасы Басқару сервері қызметінің есептік жазбасына қажетті жүйелік құқықтарын тағайындайды.

Орнату аяқталғаннан кейін, Сервер дерекқоры жасалады және барлық қажетті жүйелік құқықтар Басқару сервері қызметінің есептік жазбасына тағайындалады. Басқару сервері жұмыс істеуге дайын.

Сіз *master* дерекқорына байланыстырудың күшін жоя аласыз, себебі Басқару серверін орнату кезінде орнату бағдарламасы Сервер дерекқорын жасап, осы дерекқормен салыстыруды конфигурациялады.

Дерекқорды автоматты түрде жасау үшін Басқару серверімен күнделікті жұмыс істеуге қарағанда көбірек рұқсаттар қажет болғандықтан, кейбір рұқсаттарды қайтарып алуыңызға болады. SQL Server серверінде SQL Server есептік жазбасын таңдап, Басқару серверімен жұмыс істеу үшін келесі құқықтарды беріңіз:

- Сервер деңгейінің рөлі: public.
- Сервер дерекқоры үшін дерекқор мүшелігінің рөлі: db_owner.
- Сервер дерекқорының әдепкі бойынша схемасы: dbo.
- Рұқсаттар:
  - CONNECT SQL
  - VIEW ANY DATABASE

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын қолмен жасау)

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. SQL Server серверінде бос дерекқор жасаңыз. Бұл дерекқор Басқару сервері дерекқоры ретінде пайдаланылады.

2. SQL Server серверінде, SQL Server есептік жазбасына келесі құқықтар мен рұқсаттар беріңіз:
   - Сервер деңгейінің рөлі: public.
   - Дерекқор жасау үшін дерекқор мүшелігі рөлі: db_owner.
   - Дерекқор жасау үшін әдепкі бойынша схема: dbo.
   - Рұқсаттар:
     - CONNECT SQL
     - VIEW ANY DATABASE

3. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасымен жүйеге кіріңіз.
4. Орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
5. Басқару серверінің таңдаулы орнатылымын таңдаңыз.
6. Басқару сервері дерекқоры сақталатын ДҚБЖ ретіндегі Microsoft SQL Server тармағын таңдаңыз.
7. Құрылған дерекқордың атауын Басқару сервері дерекқорының атауы ретінде көрсетіңіз.
8. Жасалған SQL Server есептік жазбасының көмегімен Басқару сервері мен SQL Server арасында қосылым орнату үшін SQL Server түпнұсқалық растамасы режимі тармағын таңдаңыз. Содан соң, SQL Server есептік жазбасы деректерін көрсетіңіз.
9. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

   Сіз бар Windows пайдаланушы есептік жазбасын таңдай аласыз немесе орнату бағдарламасын пайдаланып, KL-AK-* Windows есептік жазбасын жасай аласыз. Таңдалған есептік жазбаға қарамастан, орнату бағдарламасы Басқару сервері қызметінің есептік жазбасына қажетті жүйелік құқықтарын тағайындайды.

Орнату аяқталғаннан кейін, Басқару сервері Басқару серверінің деректерін сақтау үшін құрылған дерекқорды пайдаланады. Барлық қажетті жүйелік құқықтар Басқару сервері қызметінің есептік жазбасына тағайындалады. Басқару сервері жұмыс істеуге дайын.

MySQL және MariaDB жүйесімен жұмыс істеу үшін есептік жазбаларды конфигурациялау

Алдын ала талаптар

Есептік жазбаларға құқықтарды тағайындамас бұрын келесі әрекеттерді орындаңыз:

1. Жергілікті әкімші есептік жазбасымен кіргеніңізге көз жеткізіңіз.
2. MySQL немесе MariaDB жүйесімен жұмыс істеу үшін ортаны орнатыңыз.
3. Басқару сервері орнатылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.
4. Басқару сервері қызметі іске қосылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. ДҚБЖ орнату кезінде жасаған root тіркелгісінде MySQL немесе MariaDB жұмыс ортасын іске қосыңыз.

2. Құпиясөзі бар ішкі ДҚБЖ есептік жазбасын жасаңыз. Басқару сервері қызметі және Басқару серверін орнату бағдарламасы (бұдан әрі - орнату бағдарламасы) ДҚБЖ-не қатынасу үшін осы ДҚБЖ ішкі есептік жазбасын пайдаланады. Осы есептік жазбаға келесі құқықтар беріңіз:

   - Артықшылықтар схемасы:
     - Басқару сервері дерекқоры: ALL (`GRANT OPTION` қоспағанда).
     - Жүйе схемалары (mysql және sys): `SELECT`, `SHOW VIEW`.
     - Sys.table_exists сақталатын рәсімі: `EXECUTE`.
   - Барлық схемаларға арналған жаһандық артықшылықтар: `PROCESS`, `SUPER`.

   Ішкі ДҚБЖ есептік жазбасын жасау және осы есептік жазбаға қажетті құқықтарды беру үшін, төмендегі скриптті іске қосыңыз (бұл скриптте ДҚБЖ есептік жазбасы – *KSCAdmin*, ал Басқару сервері дерекқоры атауы – *kav*):

```
/* KSCAdmin атауы бар пайдаланушыны жасау */
CREATE USER 'KSCAdmin'
/* KSCAdmin үшін құпиясөз көрсету */
IDENTIFIED BY '<құпиясөз>';
```

   ДҚБЖ ретінде MySQL 8.0 немесе одан бұрынғы нұсқасын пайдалансаңыз, бұл нұсқалар үшін "SHA2 құпиясөзін кэштеу" аутентификациясына қолдау көрсетілмейтінін ескеріңіз. Әдепкі аутентификацияны "SHA2 құпиясөзін кэштеу" күйінен "MySQL жеке құпиясөзі" параметріне өзгертіңіз:

   - "MySQL жеке құпиясөзі" пайдаланып ДҚБЖ есептік жазбасын жасау үшін келесі пәрменді орындаңыз:
     `CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<құпиясөз>';`
   - Қолданыстағы ДҚБЖ есептік жазбасының аутентификациясын өзгерту үшін келесі пәрменді орындаңыз:
     `ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<құпиясөз>';`

```
/* KSCAdmin артықшылықтарын ұсыну */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

MariaDB 10.5 немесе одан бұрынғы нұсқасын ДҚБЖ ретінде пайдалансаңыз, сізге EXECUTE құқығын берудің қажеті жоқ. Бұл жағдайда скриптіден келесі пәрменді алып тастаңыз: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. ДҚБЖ есептік жазбасына берілген артықшылықтар тізімін көру үшін келесі скриптті іске қосыңыз:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Басқару серверінің дерекқорын қолмен жасау үшін, келесі скриптті іске қосыңыз (бұл скриптте Басқару серверінің дерекқорының атауы – *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Сондай-ақ, ДҚБЖ есептік жазбасын жасайтын сценарийде көрсеткен дерекқордың атауын пайдаланыңыз.

5. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасымен жүйеге кіріңіз.

6. Орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

7. Басқару серверінің таңдаулы орнатылымын таңдаңыз.

8. Басқару серверінің дерекқоры сақталатын ДҚБЖ ретіндегі Microsoft MySQL немесе MariaDB тармағын таңдаңыз.

9. Басқару серверінің дерекқорының атауын көрсетіңіз. Скриптте көрсетілген дерекқордың атауын пайдаланыңыз.

10. Скрипттің көмегімен жасалған ДҚБЖ есептік жазбасының есептік деректерін көрсетіңіз.

11. Басқару серверінің қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

    Сіз бар Windows пайдаланушы есептік жазбасын таңдай аласыз немесе орнату бағдарламасын пайдаланып, автоматты түрде KL-AK-* Windows есептік жазбасын жасай аласыз. Таңдалған есептік жазбаға қарамастан, орнату бағдарламасы Басқару серверінің қызметінің есептік жазбасына қажетті жүйелік құқықтарын тағайындайды.

Орнату аяқталғаннан кейін, Басқару серверінің дерекқоры құрылады және Басқару сервері жұмыс істеуге дайын.

Деректерді MySQL және MariaDB ДҚБЖ-лардағы ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу

MySQL және MariaDB ДҚБЖ үшін деректерді келесі жолдармен сақтауға болады:

- Барлық пайдаланушы дерекқорының деректері бір файлда (әдетте `ibdata1` файлында) сақталған кезде, ортақ кесте кеңістігі ретінде.
- Әр кесте үшін бөлек деректер кеңістігі жеке файл ретінде жасалғанда, әр кестедегі файл кеңістігі ретінде.

Ортақ кесте кеңістігін пайдалану кесте кеңістігінің фрагментациялану қаупін арттырады. `SHRINK` мүмкін болмағандықтан, ортақ кесте кеңістігіндегі файл диск кеңістігінің шамамен 90%-ын алуы мүмкін. Бұл дискінің ішкі жүйесінің жұмысына теріс әсер етеді. Осылайша әр кестедегі файл кеңістігін таңдау пайдалы.

Бұл мақалада деректерді ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу жолы сипатталған. MySQL немесе MariaDB ДҚБЖ басқа қолданбалармен де пайдаланылса, осы қолданбалардың дерекқорларын әр кестедегі файл кеңістігіне жіберу керек.

> Бұл процедураны тек Басқару сервері үшін MySQL немесе MariaDB ДҚБЖ пайдалансаңыз ғана орындауды ұсынамыз.
> Деректерді ортақ кестелік кеңістіктен жеке файлдық кестелік кеңістікке жылжыту диск ішкі жүйесіне жүктемені арттыруы мүмкін.

Алдын ала талаптар

Бастамай тұрып, келесілерді тексеріңіз:

- Деректердің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын іске қосу арқылы басқару сервері деректерінің сақтық көшірмесін жасадыңыз.
- Дерекқорлары MySQL немесе MariaDB ДҚБЖ (бар болса) арқылы басқарылатын басқа қолданбалардың сақтық көшірмесін жасадыңыз.
- ДҚБЖ орнатылған құрылғыда дерекқор бар бөлімде бос диск кеңістігі бар.

Қажетті диск кеңістігі ағымдағы жалпы дерекқорлар өлшемінің 150%-ын құрайды (`ibdata1` файлының ағымдағы өлшемі).

Процесс

Деректерді ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберу үшін:

1. Осы процедураны орындағыңыз келетін ДҚБЖ данасын пайдаланып, Kaspersky Security Center басқару сервері қызметін және басқа қолданбаларды тоқтатыңыз.
2. ДҚБЖ нұсқасына байланысты ДҚБЖ-ға суперпайдаланушы ретінде кіріңіз, содан кейін кез келген ыңғайлы қолданбада `fix_tablespace.sql` скриптісін іске қосыңыз.

   Осы сілтемелерді басып, `fix_tablespace.sql` скриптілерін көруге болады:

   MySQL 5.7 және MariaDB 10.1+ скриптісін көру

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
```

```
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

MySQL 8.0+ үшін скриптіні көру

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Скриптінің орындалуын тоқтатпау керек.
Ешбір ДҚБЖ қатесі орын алмаса, бірақ скриптінің орындалуын тоқтатсаңыз, скриптіні қайта іске қосыңыз немесе осы процедураның қадамдарын орындауды тоқтатыңыз, ДҚБЖ қызметін қайта іске қосыңыз және сақтық көшірмеден басқару серверінің деректерін қалпына келтіріңіз.

3. my.cnf файлының `[mysqld]` бөлімінде `innodb_file_per_table` параметрін `1` мәніне орнатыңыз.

4. MySQL немесе MariaDB қызметін қайта іске қосыңыз.

5. Kaspersky Security Center басқару сервері қызметін қайта іске қосыңыз.

Деректер ортақ кесте кеңістігінен әр кестедегі файл кеңістігіне жіберіледі.

PostgreSQL және Postgres Pro жүйесімен жұмыс істеу үшін есептік жазбаларды конфигурациялау

Алдын ала талаптар

Есептік жазбаларға құқықтарды тағайындамас бұрын келесі әрекеттерді орындаңыз:

1. Жергілікті әкімші есептік жазбасымен кіргеніңізге көз жеткізіңіз.
2. PostgreSQL және Postgres Pro-мен жұмыс істеу үшін ортаны орнатыңыз.
3. Kaspersky Security Center 15.1 бағдарламасымен жұмыс істеу үшін PostgreSQL немесе Postgres Pro серверін конфигурациялау.
4. Басқару сервері орнатылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.
5. Басқару сервері қызметі іске қосылатын Windows есептік жазбаңыз бар екеніне көз жеткізіңіз.

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын автоматты түрде жасау)

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. PostgreSQL және Postgres Pro-мен жұмыс істеу үшін ортаны іске қосыңыз.
2. ДҚБЖ жүйесіне кіру үшін Postgres рөлін таңдаңыз. Сіз келесі рөлдердің бірін пайдалана аласыз:
   - *Postgres* пайдаланушысы (әдепкі бойынша Postgres рөлі).

     Егер сіз *Postgres* пайдаланушысын қолдансаңыз, оған қосымша құқықтар берудің қажеті жоқ.
   - Postgres жаңа рөлі.

     Егер сіз жаңа Postgres рөлін пайдаланғыңыз келсе, сол рөлді жасаңыз және оған CREATEDB құқығын беріңіз. Ол үшін келесі скриптті іске қосыңыз (бұл скриптте *KSCAdmin* мәні рөлге ие):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
     ```

     Жасалған рөл Басқару сервері дерекқорының иесі ретінде пайдаланылады (бұдан әрі - Сервер дерекқоры).
3. Басқару серверін орнату бағдарламасы (бұдан әрі - орнатушы) іске қосылған Windows есептік жазбасының астынан жүйеге кіріңіз.
4. Орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

5. Басқару серверінің таңдаулы орнатылымын таңдаңыз.

6. Басқару сервері дерекқоры сақталатын ДҚБЖ ретіндегі PostgreSQL немесе Postgres Pro тармағын таңдаңыз.

7. Сервер дерекқорының атауын көрсетіңіз. Орнату бағдарламасы автоматты түрде Сервер дерекқорын жасайды.

8. Postgres рөлінің есептік деректерін көрсетіңіз.

9. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

   Сіз бар Windows пайдаланушы есептік жазбасын таңдай аласыз немесе орнату бағдарламасын пайдаланып, автоматты түрде KL-AK-* Windows есептік жазбасын жасай аласыз. Таңдалған есептік жазбаға қарамастан, орнату бағдарламасы Басқару сервері қызметінің есептік жазбасына қажетті жүйелік құқықтарын тағайындайды.

Орнату аяқталғаннан кейін, Сервер дерекқоры автоматты түрде жасалады және Басқару сервері жұмыс істеуге дайын.

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау (Басқару серверінің дерекқорларын қолмен жасау)

Басқару серверін орнату үшін есептік жазбаларды конфигурациялау үшін:

1. Postgres-пен жұмыс істеу үшін ортаны іске қосыңыз.

2. *Postgres* дерекқорындағы *Postgres* пайдаланушысымен кіріңіз.

3. Жаңа Postgres рөлін жасаңыз (бұл мысалда рөл — *KSCAdmin*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
   ```

4. Басқару серверінің дерекқорын жасаңыз (бұл мысалда Басқару сервері дерекқорының атауы – *KAV*):

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   Егер сіз "New encoding (UTF8) is incompatible with the encoding of the template database" қатесін алсаңыз, пәрменді пайдаланып дерекқорды жасаңыз:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   осының орнына:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Содан кейін рөлге басқару сервері дерекқорындағы барлық артықшылықты тағайындаңыз:

```
GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
```

Басқару сервері дерекқорында рөлдің әдепкі ҚОСЫЛУ және УАҚЫТША артықшылықтары бар екеніне көз жеткізіңіз.

6. Жасалған Postgres рөліне келесі құқықтарды беріңіз:

- Жалпыға ортақ схемадағы барлық кестелерге қатынасу құқықтары: ALL.
- Жалпыға ортақ схемадағы барлық бірізділіктерге қатынасу құқықтары: ALL.

Ол үшін сервер дерекқорына *Postgres* пайдаланушысы ретінде кіріңіз және келесі скриптіні іске қосыңыз (бұл скриптіде рөл — *KSCAdmin*):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
```

7. Орнату бағдарламасын іске қосу үшін пайдаланылатын Windows есептік жазбасымен жүйеге кіріңіз.
8. Басқару серверін орнату бағдарламасын іске қосыңыз.

   Басқару серверін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
9. Басқару серверінің таңдаулы орнатылымын таңдаңыз.
10. Басқару сервері дерекқоры сақталатын ДҚБЖ ретіндегі PostgreSQL немесе Postgres Pro тармағын таңдаңыз.
11. Сервер дерекқорының атауын көрсетіңіз. Скриптте көрсетілген дерекқордың атауын пайдаланыңыз. Дерекқор атауын енгізген кезде әріптер тіркелімін ескеріңіз.
12. Postgres рөлінің есептік деректерін көрсетіңіз.
13. Басқару сервері қызметін іске қосу үшін қолданылатын Windows есептік жазбасын көрсетіңіз.

    Сіз бар Windows пайдаланушы есептік жазбасын таңдай аласыз немесе орнату бағдарламасын пайдаланып, автоматты түрде KL-AK-* Windows есептік жазбасын жасай аласыз. Таңдалған есептік жазбаға қарамастан, орнату бағдарламасы Басқару сервері қызметінің есептік жазбасына қажетті жүйелік құқықтарын тағайындайды.

Орнату аяқталғаннан кейін, Басқару сервері Басқару серверінің деректерін сақтау үшін құрылған дерекқорды пайдаланады. Басқару сервері жұмыс істеуге дайын.

Microsoft SQL Server түпнұсқалық растамасы

Бұл бөлімдегі ақпарат Kaspersky Security Center бағдарламасы Microsoft SQL Server серверін дерекқорларды басқару жүйесі ретінде қолданатын конфигурацияларға ғана қолданылады.

Дерекқорға немесе одан берілетін Kaspersky Security Center деректерін, сондай-ақ дерекқорда сақталатын деректерді рұқсатсыз қатынасудан қорғау үшін, сіз Kaspersky Security Center бағдарламасы мен SQL Server сервері арасындағы байланысты қорғауыңыз керек. Қауіпсіз байланысты қамтамасыз етудің ең сенімді тәсілі - Kaspersky Security Center бағдарламасы мен SQL Server серверін бір құрылғыда орнату және екі бағдарлама үшін де бірлескен жад механизмін қолдану. Барлық жағдайларда, біз SQL Server үлгісінің түпнұсқалық растамасы үшін SSL немесе TLS сертификатын пайдалануды ұсынамыз. Сенімді сертификаттау орталығының (CA) сертификатын немесе өздігінен қол қойылған сертификатты қолдана аласыз. Сенімді сертификаттау орталығының сертификатын қолдану ұсынылады, себебі өздігінен қол қойылған сертификат тек шектеулі қорғанысты қамтамасыз етеді.

SQL Server түпнұсқалық растамасы келесі кезеңдерден тұрады:

1. **SQL Server сервері үшін өздігінен қол қойылған SSL немесе TLS сертификатын сол сертификаттың талаптарына сай жасау**

   SQL Server үшін сертификатыңыз әлдеқашан бар болса, бұл қадамды өткізіп жіберіңіз.

   SSL сертификатын тек SQL Server серверінің 2016 жылдан бұрынғы нұсқаларына (13.x) ғана қолдануға болады. SQL Server 2016 (13.x) және одан жоғары нұсқаларында TLS сертификатын қолданыңыз.

   Мысалы, TLS сертификатын жасау үшін PowerShell-де келесі пәрменді енгізіңіз:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   > Үлгі доменге енгізілген болса, пәрмен жолында SQL_HOST_NAME ретінде SQL Server үлгісінің атын енгізу керек немесе үлгі доменге енгізілмеген болса, үлгінің *толық домендік атауын* (FQDN) енгізу қажет. Басқару серверін орнату шеберінде SQL Server үлгісі атауы ретінде дәл сол атау – үлгі атауы немесе толық домендік атау көрсетілуі тиіс.

2. **SQL Server үлгісіне арналған сертификатты қосу**

   Бұл кезеңнің нұсқаулары SQL Server жұмыс істейтін платформаға байланысты. Кеңейтілген ақпаратты ресми құжаттамадан қараңыз:

   - Windows
   - Linux
   - Amazon реляциялық дерекқорлар қызметі

   Істен шығуға төзімді кластерде сертификатты қолдану үшін, істен шығуға төзімді кластердің әрбір түйінінде сертификатты орнату керек. Толығырақ ақпарат алу үшін Microsoft құжаттамасын қараңыз.

3. **Қызметтің есептік жазбасы үшін рұқсаттар тағайындау**

   SQL Server қызметі іске қосылатын қызметтің есептік жазбасы жеке кілттерге қатынасу үшін "Толық қатынас" рұқсатына ие. Толығырақ ақпарат алу үшін Microsoft құжаттамасын қараңыз.

4. **Сертификатты Kaspersky Security Center үшін сенімді сертификаттар тізіміне қосу**

   Басқару сервері құрылғысына сертификатты сенімді сертификаттар тізіміне қосыңыз. Толығырақ ақпарат алу үшін Microsoft құжаттамасын қараңыз.

5. **SQL Server үлгісі мен Kaspersky Security Center арасындағы шифрланған қосылымдарды қосу**

   Басқару сервері құрылғысында `KLDBADO_UseEncryption` айнымалы ортасы үшін `1` мәнін орнатыңыз. Мысалы, Windows Server 2012 R2 жүйесінде **Жүйенің сипаттары** терезесінің **Қосымша** қойындысында **Айнымалы орталар** түймесін басып, айнымалы орталарды өзгерте аласыз. `KLDBADO_UseEncryption` атты айнымалыны қосып, `1` мәнін орнатыңыз.

6 **1.2 TLS-протоколын қолдану үшін қосымша конфигурация**

1.2 TLS-протоколын қолдансаңыз, қосымша түрде келесі әрекеттерді орындаңыз:

- SQL Server орнатылған нұсқасы 64 разрядты бағдарлама екеніне көз жеткізіңіз.
- Microsoft OLE DB драйверін Басқару сервері құрылғысына орнатыңыз. Толығырақ ақпарат алу үшін Microsoft құжаттамасын қараңыз.
- Басқару сервері құрылғысында `KLDBADO_UseMSOLEDBSQL` айнымалы ортасы үшін `1` мәнін орнатыңыз. Мысалы, Windows Server 2012 R2 жүйесінде **Жүйенің сипаттары** терезесінің **Қосымша** қойындысында **Айнымалы орталар** түймесін басып, айнымалы орталарды өзгерте аласыз. `KLDBADO_UseMSOLEDBSQL` атты жаңа айнымалыны қосып, `1` мәнін орнатыңыз.

  OLE DB драйверінің нұсқасы 19 немесе одан жоғары болса, `KLDBADO_ProviderName` ортасының айнымалы мәнін `MSOLEDBSQL19` етіп орнатыңыз.

7 **TCP/IP протоколын SQL Server атаулы үлгісінде қолдануды қосу**

Сіз SQL Server атаулы үлгісін қолдансаңыз, қосымша түрде TCP/IP протоколын қолдануды қосыңыз және SQL Server Database Engine құрамдасы үшін TCP/IP порты нөмірін тағайындаңыз. Басқару серверін орнату шеберінде SQL Server серверіне қосылымды конфигурациялау кезінде, **SQL Server үлгісінің атауы** өрісінде SQL Server үлгісінің атауы мен порт нөмірін көрсетіңіз.

Сценарий: MySQL Server серверінің аутентификациясы

MySQL серверінің аутентификациясы үшін TLS сертификатын пайдалану ұсынылады. Сенімді сертификаттау орталығының (CA) сертификатын немесе өздігінен қол қойылған сертификатты қолдана аласыз.

Басқару сервер MySQL үшін бір жақты және екі жақты SSL аутентификациясына қолдау көрсетеді.

Бір жақты SSL аутентификациясын қосу

MySQL үшін бір жақты SSL аутентификациясын орнату мақсатында мына қадамдарды орындаңыз:

1. **MySQL сервері үшін өздігінен қол қойылған TLS сертификатын жасау.**

   PowerShell бағдарламасындағы орынды сертификаттарды сақтағыңыз келетін қалтамен ауыстырыңыз. Келесі пәрмендерді орындаңыз:

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

   Бұл пәрмендер ағымдағы пайдаланушы үшін куәліктер жасайды және сертификаттарды PEM пішіміне экспорттайды. Сервердің аутентификациясы үшін сізге тек экспортталған PEM файлдары қажет. Жасалған сертификаттарды Windows жүйесінен жою үшін PowerShell бағдарламасында келесі пәрменді іске қосыңыз:

```
certmgr.msc
```

   Жасалған сертификаттарды **Жеке** → **Сертификаттар** қалтасынан тауып, оларды жойыңыз.

2. **Сервер жалаушасының файлын жасау**

Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Klscflag утилитасын пайдаланып, KLSRV_MYSQL_OPT_SSL_CA сервері жалаушасын жасаңыз және оның мәндері ретінде сертификатқа жолды көрсетіңіз:

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <жолы: ca-cert.pem> -t s
```

3. **Дерекқорды конфигурациялаңыз**

   my.cnf файлында сертификаттарды көрсетіңіз. Мәтіндік редакторда my.cnf файлын ашыңыз және [mysqld] бөліміне келесі жолдарды қосыңыз:

   ```
   [mysqld]
   ssl-ca="...\mysqlcerts\ca-cert.pem"
   ssl-cert="...\mysqlcerts\server-cert.pem"
   ssl-key="...\mysqlcerts\server-key.pem"
   ```

Екі жақты SSL аутентификациясын қосу

MySQL үшін екі жақты SSL аутентификациясын орнату мақсатында мына қадамдарды орындаңыз:

1. **Сервер жалауша файлдарын жасау**

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Klscflag утилитасын пайдаланып, сервер жалаушаларын жасаңыз және олардың мәндері ретінде сертификат файлдарына жолды көрсетіңіз:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <жолы: ca-cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <жолы: server-cert.pem> -t
   s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <жолы: server-key.pem> -t s
   ```

2. **Құпия сөйлемді көрсетіңіз (міндетті емес)**

   Егер server-key.pem кодты сөйлемді қажет етсе, KLSRV_MARIADB_OPT_TLS_PASPHRASE жалаушасын жасаңыз және кодты сөйлемді оның мәні ретінде көрсетіңіз:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <кодты сөйлем> -t s
   ```

3. **Дерекқорды конфигурациялаңыз**

   my.cnf файлында сертификаттарды көрсетіңіз. Мәтіндік редакторда my.cnf файлын ашыңыз және [mysqld] бөліміне келесі жолдарды қосыңыз:

   ```
   [mysqld]
   ssl-ca="...\ca-cert.pem"
   ssl-cert="...\server-cert.pem"
   ssl-key="...\server-key.pem"
   ```

Сценарий: PostgreSQL Server серверінің аутентификациясы

PostgreSQL серверінің аутентификациясы үшін TLS сертификатын пайдалану ұсынылады. Сенімді сертификаттау орталығының (CA) сертификатын немесе өздігінен қол қойылған сертификатты қолдана аласыз. Сенімді сертификаттау орталығының (CA) сертификатын қолдану ұсынылады, себебі өздігінен қол қойылған сертификат тек шектеулі қорғанысты қамтамасыз етеді.

Басқару сервер PostgreSQL үшін бір жақты және екі жақты SSL аутентификациясына қолдау көрсетеді.

PostgreSQL серверінің аутентификациясы кезең-кезеңімен жүзеге асырылады:

1. **PostgreSQL сервері үшін сертификат жасау**

   OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрмендерді орындаңыз:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **Басқару сервері үшін сертификат жасау**

   Келесі пәрмендерді орындаңыз. CN мәні Басқару сервер атынан PostgreSQL-ге қосылатын пайдаланушының атына сәйкес болуы керек. Әдепкі пайдаланушы аты - postgres.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **Клиент сертификатының аутентификациясын конфигурациялау**

   pg_hba.conf келесідей өзгертіңіз:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   pg_hba.conf ішінде `host` деп басталатын жазба жоқ екеніне көз жеткізіңіз.

4. **PostgreSQL сертификатын көрсету**

   Бір жақты SSL аутентификациясы

   postgresql.conf файлын келесідей өзгертіңіз (.crt және .key файлдарына дұрыс жолды көрсетіңіз):

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   Екі жақты SSL аутентификациясы

   postgresql.conf файлын келесідей өзгертіңіз (.crt және .key файлдарына дұрыс жолды көрсетіңіз):

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **PostgreSQL демонын қайта іске қосу**

   Келесі пәрменді орындаңыз:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Басқару сервері үшін сервер жалаушасын көрсету**

   Бір жақты SSL аутентификациясы

   Klscflag утилитасын пайдаланып, KLSRV_POSTGRES_OPT_SSL_CA сервері жалаушасын жасаңыз және оның мәндері ретінде сертификатқа жолды көрсетіңіз:

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Келесі пәрменді орындаңыз:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <жолы: psql.crt> -t s
   ```

   Екі жақты SSL аутентификациясы

   Klscflag утилитасын пайдаланып, сервер жалаушаларын жасаңыз және олардың мәндері ретінде сертификат файлдарына жолды көрсетіңіз.

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Келесі пәрмендерді орындаңыз:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <жолы: psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <жолы: postgres.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <жолы: postgres.key> -t s
   ```

   Егер `postgres.key` кодты сөйлемді қажет етсе, KLSRV_POSTGRES_OPT_TLS_PASPHRASE жалаушасын жасаңыз және кодты сөйлемді оның мәні ретінде көрсетіңіз:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <құпиясөз тіркесі> -t s
   ```

7. **Басқару сервері қызметін қайта іске қосу**

Басқару серверін орнату бойынша ұсыныстар

Осы бөлімде Басқару серверін орнатуға қатысты ұсынымдар бар. Бөлімде клиент құрылғыларында Желілік агентті орналастыруға арналған Басқару серверін қамтитын құрылғыда ортақ қатынасы бар қалталарды қолдану сценарийлері де бар.

Істен шығуға төзімді кластерде Басқару серверінің қызметтеріне арналған есептік жазбалар жасау

Әдепкі бойынша инсталлятор Басқару серверінің қызметтері үшін ерекше артықшылығы жоқ есептік жазбаларды өз бетінше жасайды. Мұндай жүріс-тұрыс Басқару серверін кәдімгі құрылғыға орнату үшін анағұрлым қолайлы.

Алайда Басқару серверін істен шығуға төзімді кластерге орнатқан кезде басқаша жасау керек:

1. Басқару серверінің қызметтері үшін ерекше артықшылығы жоқ домендік есептік жазбалар жасау және оларды KLAdmins жаһандық домендік қауіпсіздік тобының мүшелеріне айналдыру.

2. Басқару серверінің инсталляторында қызметтер үшін жасалған домендік есептік жазбаларды белгілеу.

Ортақ қатынасы бар қалтаны белгілеу

Басқару серверін орнатқан уақытта ортақ қатынасы бар қалтаның орналасқан жерінбелгілеуге болады. Ортақ қатынасы бар қалтаның орналасқан жерін орнатқан соң, Басқару серверінің сипаттарында белгілеуге болады. Әдепкі бойынша ортақ қатынасы бар қалта Басқару сервері бар құрылғыда жасалады (**Everyone**кіріктірілген тобы үшін оқуға арналған қатынаспен). Алайда кейбір жағдайларда (жоғары жүктеме немесе оқшауланған желіден қатынасу қажеттілігі сияқты) ортақ қатынасы бар қалтаны мамандандырылған файлдық ресурсқа орналастырған жөн.

Ортақ қатынасы бар қалта Желілік агентті орналастырудың бірнеше сценарийінде пайдаланылады.

Ортақ қатынасы бар қалта үшін тіркелімді есепке алу сөндірілуі тиіс.

Active Directory топтық саясаттары көмегімен Басқару серверінің құралдарымен қашықтағы орнату

Егер құрылғылар Windows доменінде болса (жұмыс топтары жоқ), бастапқы орналастыруды (әлі басқарылмайтын құрылғыларға Желілік агентті және қауіпсіздік бағдарламасын орнату) Active Directory топтық саясаттары көмегімен орындаған жөн. Орналастыру Kaspersky Security Center қашықтағы инсталляциясының штаттық тапсырмасы көмегімен орындалады. Егер желі өлшемі үлкен болса, Басқару сервері бар құрылғының дискілі ішкі жүйесіне жүктемені азайту үшін ортақ қатынасы бар қалтаны мамандандырылған файлдық ресурсқа орналастырған жөн.

Автономды пакетке UNC-жолын тарату арқылы қашықтан орнату

Егер ұйым желісінің құрылғыларын пайдаланушылар жергілікті әкімшінің құқықтарына ие болса, бастапқы орналастырудың тағы бар тәсілі – Желілік агенттің автономды пакетін жасау (немесе тіпті қауіпсіздік бағдарламасымен бірге Желілік агенттің "қосарланған" пакетін) болып табылады. Автономды пакетті жасаудан кейін желі құрылғыларының пайдаланушыларына ортақ қатынасы бар қалтадағы пакетке сілтемені жіберу керек. Инсталляция сілтеме бойынша іске қосылады.

Басқару серверінің ортақ қатынасы бар қалтасынан жаңарту

Антивирусты жаңарту тапсырмасында Басқару серверінің ортақ қатынасы бар қалтасынан жаңартуды конфигурациялауға болады. Егер тапсырма құрылғылардың көбірек саны үшін тағайындалса, ортақ қатынасы бар қалтаны мамандандырылған файлдық ресурсқа орналастырған жөн.

Операциялық жүйенің кескіндерін орнату

Операциялық жүйелердің үлгілерін орнату әрдайым ортақ қатынасы бар қалтаны қолданып орындалады: құрылғылар қалтадан операциялық жүйелердің үлгілерін оқиды. Егер ұйымның құрылғыларының көбірек санында үлгілерді орналастыру жоспарланса, онда ортақ қатынасы бар қалтаны мамандандырылған файлдық ресурсқа орналастырған жөн.

Басқару серверінің мекенжайын көрсету

Басқару серверін орнатқан кезде Басқару серверінің мекенжайын белгілеуге болады. Бұл мекенжай, әдепкі бойынша Желілік агенттің орнату пакеттерін жасау кезінде қолданылады.

Басқару серверінің мекенжайы ретінде мыналарды көрсете аласыз:

- NetBIOS-әдепкі бойынша көрсетілген Басқару серверінің атауы.
- Егер ұйымның желісінде домендік атаулар жүйесі (DNS) конфигурацияланса және тиісінше жұмыс істесе, Басқару серверінің толық домендік атауы (FQDN).
- Егер Басқару сервері демилитаризацияланған аймаққа (DMZ) орнатылса, сыртқы мекенжай.

Алдағыда, Басқару серверінің мекенжайын Басқару консолі арқылы өзгертуге болады, бірақ бұл арада ол қазірдің өзінде жасалған Желілік агенттің орнату пакеттерінде автоматты түрде өзгермейді.

Стандартты орнату

Стандартты орнату – бағдарлама файлдары үшін әдепкі бойынша белгіленген жолдар пайдаланылатын, әдепкі бойынша плагиндер жиынтығы орнатылатын және Ұялы құрылғыларды басқару қосылмайтын Басқару серверін орнату.

Жергілікті құрылғыға Kaspersky Security Center Басқару серверін орнату үшін,

орындалатын ksc_<нұсқа нөмірі>.<жинақ нөмірі>_full_<локализация тілі>.exe файлын іске қосыңыз.

Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. **Kaspersky Security Center Басқару серверін орнату** сілтемесі бойынша бағдарламалар таңдалатын терезеде Басқару серверін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

1-қадам. Лицензиялық келісім мен Құпиялық саясатын қарап шығу

Орнату шеберінің осы қадамында, сіз бен Kaspersky арасында жасалатын Лицензиялық келісім және Құпиялылық саясатымен танысу қажет.

Сондай-ақ, сізден Kaspersky Security Center дистрибутивінде қолжетімді бағдарламаларды басқару плагиндеріне Лицензиялық келісімдермен және Құпиялылық саясаттарымен танысу сұралуы мүмкін.

Сіз бен Kaspersky арасында жасалатын Лицензиялық келісімді және Құпиялылық саясатын мұқият оқып шығыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз, мұны тиісті жалаушаларды белгілеу арқылы растаңыз.

Бағдарламаны орнату келесі екі жалаушаны қойғаннан кейін жалғасады.

Лицензиялық келісіммен немесе Құпиялылық саясатымен келіспесеңіз, **Бас тарту** түймесін басып, бағдарламаны орнатуды болдырмаңыз.

2-қадам. Орнату түрі таңдау

Орнату түрін таңдау терезесінде **Стандартты** түрін көрсетіңіз.

Kaspersky Security Center бағдарламасымен танысқыңыз келсе, мысалы, оның жұмысын ұйымыңыздың желісінің шағын бөлігінде сынағыңыз келсе, стандартты орнату тәсілі ұсынылады. Стандартты орнату кезінде сіз тек дерекқор параметрлерін конфигурациялайсыз. Басқару серверінің параметрлері конфигурацияланбайды, олар үшін әдепкі бойынша белгіленген мәндер қолданылады. Стандартты орнату сізге орнатылатын басқару плагиндерін таңдауға мүмкіндік бермейді, әдепкі бойынша белгіленген плагиндер жиынтығы орнатылады. Стандартты орнату кезінде ұялы құрылғыларға арналған орнату пакеттері жасалмайды. Оларды кейінірек Басқару консолінде жасауға болады.

3-қадам. Kaspersky Security Center Web Console орнату

64 разрядты операциялық жүйені қолдансаңыз, бұл қадам көрсетілмейді. Әйтпесе, бұл қадам көрсетілмейді, өйткені Kaspersky Security Center Web Console веб-консолі 32 разрядты операциялық жүйелермен жұмыс істемейді.

Әдепкі бойынша, Kaspersky Security Center Web Console және Microsoft Management Console (MMC) негізіндегі Басқару консолі орнатылады.

Kaspersky Security Center Web Console веб-консолін ғана орнатқыңыз келсе:

1. **Консольдердің бірін орнату тармағын** таңдаңыз.
2. Ашылмалы тізімнен **Интернетке негізделген консоль** тармағын таңдаңыз.

Kaspersky Security Center Web Console орнату. Басқару серверін орнату аяқталғаннан кейін автоматты түрде іске қосылады.

Microsoft Management Console (MMC) негізінде Басқару консолін ғана орнатқыңыз келсе:

1. **Консольдердің бірін орнату тармағын** таңдаңыз.

2. Ашылмалы тізімнен **MMC негізіндегі консоль** тармағын таңдаңыз.

4-қадам. Желінің өлшемін таңдау

Kaspersky Security Center орнатылатын желінің өлшемін көрсетіңіз. Желідегі құрылғылардың санына байланысты, шебер орнату параметрлерін және бағдарлама интерфейсін көрсетуді конфигурациялайды.

Төмендегі кестеде желінің әртүрлі өлшемдерін таңдаған кезде бағдарламаны орнату және интерфейсті көрсету параметрлері атап көрсетілген.

Орнату параметрлерінің желі өлшемдерін таңдауға тәуелділігі

Параметрлер	1–100 басқарылатын құрылғы	101–1000 басқарылатын құрылғы	1001–5000 басқарылатын құрылғы	5000-нан астам басқарылатын құрылғы
Қосалқы және виртуалды басқару серверлері және консоль тармағындағы қосалқы және виртуалды басқару серверлеріне қатысты барлық параметр үшін түйінмен көрсету (MMC негізіндегі басқару консольдерінде ғана қолжетімді)	Жоқ	Жоқ	Бар	Бар
Басқару серверінің және басқару топтарының сипаттар терезелеріндегі **Қауіпсіздік** бөлімдерімен көрсету (тек MMC негізіндегі басқару консолінде қолжетімді)	Жоқ	Жоқ	Бар	Бар
Клиент құрылғыларында жаңарту тапсырмасын іске қосу уақытын кездейсоқ бөлу	Жоқ	5 минуттық аралықта	10 минуттық аралықта	10 минуттық аралықта

Басқару серверін MySQL 5.7 және SQL Express дерекқор серверіне қосқан кезде 10 000-нан астам құрылғыны басқаруға арналған бағдарламаны пайдалану ұсынылмайды. MariaDB дерекқорларын басқару жүйесі үшін басқарылатын құрылғылардың ең көп ұсынылатын саны 20 000 құрайды.

5-қадам. Дерекқорды таңдау

Шебердің осы қадамында Басқару сервері дерекқорын сақтау үшін пайдаланылатын келесі дерекқорды басқару жүйелерінің (ДҚБЖ) бірін таңдаңыз:

- **Microsoft SQL сервері немесе SQL Server Express**
- **MySQL немесе MariaDB**
- **PostgreSQL немесе Postgres Pro**

Басқару серверін домен контроллеріне емес, бөлектенген серверге орнату ұсынылады. Тек оқуға арналған домен контроллері (RODC) рөлін атқаратын серверге Kaspersky Security Center орнатсаңыз, Microsoft SQL Server (SQL Express) жергілікті түрде орнатылмауы керек (дәл сол құрылғыда). Бұл жағдайда, Microsoft SQL Server (SQL Express) серверін қашықтан (басқа құрылғыға) орнату немесе ДҚБЖ жүйесін жергілікті түрде орнату қажет болса – MySQL, MariaDB не PostgreSQL пайдалану ұсынылады.

Басқару сервері дерекқорының құрылымы Kaspersky Security Center орнату қалтасында орналасқан klakdb.chm файлында келтірілген. Бұл файл Kaspersky порталындағы келесі мұрағатта да қолжетімді: klakdb.zip.

6-қадам. SQL сервері параметрлерін конфигурациялау

Шебердің осы қадамында, өзіңіз таңдаған дерекқорды басқару жүйесіне (ДҚБЖ) байланысты, келесі қосылым параметрлерін көрсетіңіз:

- Алдыңғы қадамда **Microsoft SQL сервері немесе SQL Server Express** таңдалған болсаңыз:

  - **SQL сервері үлгісінің атауы** өрісінде, желіде орнатылған SQL серверінің атауын көрсетіңіз. **Шолу** түймесінің көмегімен, желіде орнатылған барлық SQL серверлерінің тізімін аша аласыз. Әдепкі бойынша, өріс толтырылмаған.

    SQL Server серверіне пайдаланушы порты арқылы қосылсаңыз, онда SQL Server данасының атауымен бірге порт нөмірін үтір арқылы көрсетіңіз, мысалы:

    ```
    SQL_Server_host_name,1433
    ```

    Басқару сервері мен SQL Server сервері арасындағы байланысты сертификат арқылы қорғасаңыз, **SQL сервері үлгісінің атауы** өрісінде сертификат жасау кезінде қолданылған дананың атауын көрсетіңіз. Аталған SQL Server данасын қолдансаңыз, SQL Server данасының атауымен бірге порт нөмірін үтір арқылы көрсетіңіз, мысалы:

    ```
    SQL_Server_name,1433
    ```

    Бір құрылғыда бірнеше SQL Server данасын қолдансаңыз, кері қиғаш сызық арқылы дананың атауын қосымша түрде көрсетіңіз, мысалы:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Корпоративтік желідегі SQL Server үшін Always On функциясы қосулы болса, **SQL сервері үлгісінің атауы** өрісінде қолжетімділік тобының тыңдаушысының атын енгізіңіз. Назар аударыңыз, Always On функциясы қосулы болған кезде Басқару сервері синхронды түрде бекітумен бірге қолжетімділік режимін ғана қолдайды.

  - **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

  Осы қадамда Kaspersky Security Center орнатып жатқан құрылғыға SQL серверін орнатқыңыз келсе, орнатуды доғарып, SQL серверін орнатқаннан кейін қайта іске қосуыңыз керек. Қолдау көрсетілетін SQL серверлері жүйеге қойылатын талаптарда көрсетілген.

  SQL серверін қашықтағы құрылғыға орнатқыңыз келсе, Kaspersky Security Center орнату шеберінің жұмысын тоқтатудың қажеті жоқ. SQL Server серверін орнатыңыз және Kaspersky Security Center орнатуға оралыңыз.

- Алдыңғы қадамда **MySQL немесе MariaDB** таңдалған болсаңыз:

  - **SQL сервері үлгісінің атауы** өрісінде ДҚБЖ үлгінің атауын көрсетіңіз. Әдепкі бойынша, Kaspersky Security Center орнатылатын құрылғының IP мекенжайы қолданылады.

  - **Порт** өрісінде Басқару серверін DBMS серверінің дерекқорына қосу үшін портты көрсетіңіз. Әдепкі бойынша 3306-порт орнатылған.

  - **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

- Алдыңғы қадамда **PostgreSQL немесе Postgres Pro** таңдалған болсаңыз:

  - **PostgreSQL немесе Postgres Pro сервері** өрісінде ДҚБЖ үлгінің атауын көрсетіңіз. Әдепкі бойынша, Kaspersky Security Center орнатылатын құрылғының IP мекенжайы қолданылады.

  - **Порт** өрісінде Басқару серверін ДҚБЖ-не қосу үшін портты көрсетіңіз. Әдепкі бойынша 5432-порт орнатылған.

  - **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

7-қадам. Түпнұсқалық растама режимін таңдау

Басқару серверін дерекқорларды басқару жүйесіне (ДҚБЖ) қосу кезінде қолданылатын түпнұсқалық растама режимін анықтаңыз.

Таңдалған ДҚБЖ жүйеге байланысты, сіз келесі түпнұсқалық растама режимдерін таңдай аласыз:

- SQL Express немесе Microsoft SQL Server үшін келесі нұсқалардың бірін таңдаңыз:

  - **Microsoft Windows аутентификация режимі**. Бұл жағдайда, құқықтарды тексеру кезінде Басқару серверін іске қосу үшін есептік жазба пайдаланылады.

  - **SQL серверінің аутентификация режимі**. Бұл нұсқа таңдалған жағдайда, құқықтарды тексеру үшін терезеде көрсетілген есептік жазба пайдаланылады. **Есептік жазба** және **Құпиясөз** өрістерін толтырыңыз.

    Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

  Бағдарлама дерекқордың екі түпнұсқалық растама режимі үшін қолжетімді ме екендігін тексереді. Дерекқор қолжетімді болмаса, қате туралы хабар пайда болады және сіз дұрыс есептік деректерді көрсетуіңіз қажет.

  Басқару серверінің дерекқоры басқа құрылғыда болса және Басқару серверінің есептік жазбасы дерекқордың серверіне қатынаса алмаса, онда Басқару серверін орнату немесе жаңарту кезінде SQL серверінің түпнұсқалық растамасы режимін қолданған жөн. Бұл, дерекқоры бар құрылғы доменде болмаған кезде немесе Басқару сервері LocalSystem есептік жазбасымен орнатылған жағдайда орын алуы мүмкін.

- MySQL, MariaDB, PostgreSQL немесе Postgres Pro үшін есептік жазба мен құпиясөзді көрсетіңіз.

8-қадам. Файлдарды мұрағаттан шығарып, қатты дискіге орнату

Kaspersky Security Center құрамдастарын орнату параметрлерін конфигурациялап болғаннан кейін, файлдарды қатты дискіге орнатуды іске қосуға болады.

Орнатуды іске қосу үшін қосымша бағдарламалар қажет болса, орнату шебері **Міндетті құрамдастарды орнату** терезесінде Kaspersky Security Center орнатуды бастамас бұрын хабарлайды. Қажетті бағдарламалар **Келесі** түймесін басқаннан кейін автоматты түрде орнатылады.

Соңғы бетте Kaspersky Security Center-мен жұмыс істеу үшін қандай консольді іске қосу керектігін таңдауға болады:

- **MMC негізіндегі Басқару консолін іске қосу**
- **Kaspersky Security Center Web Console консолін іске қосу**

  Бұл параметр, алдыңғы қадамдардың бірінде Kaspersky Security Center Web Console орнатуды таңдаған жағдайда ғана қолжетімді.

Сондай-ақ Kaspersky Security Center-мен жұмысты бастамай-ақ шеберді жабу үшін **Аяқтау** түймесін басуға болады. Kaspersky Security Center-мен жұмысты кейінірек кез келген уақытта бастауға болады.

Басқару консолін немесе Kaspersky Security Center Web Console веб-консолін бірінші рет іске қосу кезінде, бағдарламаны алғашқы рет конфигурациялай аласыз.

Орнату шеберінің жұмысы аяқталғаннан кейін, бағдарламаның келесі құрамдастары операциялық жүйе орнатылған қатты дискіге орнатылады:

- Басқару сервері (Желілік агентінің серверлік нұсқасымен бірге);
- Microsoft Management Console (MMC) Басқару консоліне негізделген Басқару консолі;
- Kaspersky Security Center Web Console (егер оны орнату таңдалса);
- дистрибутивте қолжетімді бағдарламаларды басқару плагиндері.

Сонымен қатар, егер бұл бағдарлама бұрын орнатылмаған болса, Microsoft Windows Installer 4.5 нұсқасы орнатылады.

Таңдаулы орнату

Таңдаулы орнату – орнату үшін құрамдастарды таңдау және бағдарлама орнатылатын қалтаны көрсету ұсынылатын Басқару серверін орнату.

Орнатудың осы түрі көмегімен, сіз дерекқор параметрлерін, Басқару сервері параметрлерін конфигурациялай аласыз, стандартты орнатуға кірмейтін құрамдастарды және Kaspersky қауіпсіздік бағдарламаларын басқару плагиндерін орната аласыз. Сондай-ақ, Ұялы құрылғыларды басқаруды да қоса аласыз.

Жергілікті құрылғыға Kaspersky Security Center Басқару серверін орнату үшін,

орындалатын ksc_<нұсқа нөмірі>.<жинақ нөмірі>_full_<локализация тілі>.exe файлын іске қосыңыз.

Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. **Kaspersky Security Center Басқару серверін орнату** сілтемесі бойынша бағдарламалар таңдалатын терезеде Басқару серверін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

1-қадам. Лицензиялық келісім мен Құпиялық саясатын қарап шығу

Орнату шеберінің осы қадамында, сіз бен Kaspersky арасында жасалатын Лицензиялық келісім және Құпиялылық саясатымен танысу қажет.

Сондай-ақ, сізден Kaspersky Security Center дистрибутивінде қолжетімді бағдарламаларды басқару плагиндеріне Лицензиялық келісімдермен және Құпиялылық саясаттарымен танысу сұралуы мүмкін.

Сіз бен Kaspersky арасында жасалатын Лицензиялық келісімді және Құпиялылық саясатын мұқият оқып шығыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз, мұны тиісті жалаушаларды белгілеу арқылы растаңыз.

Бағдарламаны орнату келесі екі жалаушаны қойғаннан кейін жалғасады.

Лицензиялық келісіммен немесе Құпиялылық саясатымен келіспесеңіз, **Бас тарту** түймесін басып, бағдарламаны орнатуды болдырмаңыз.

2-қадам. Орнату түрі таңдау

Орнату түрін таңдау терезесінде **Таңдаулы орнату** түрін көрсетіңіз.

Таңдаулы орнату тәсілі, Kaspersky Security Center параметрлерін, мысалы, ортақ қатынасы бар қалтаға апаратын жолды, есептік жазбаларды және Басқару серверіне қосылу порттары және дерекқор параметрлерін конфигурациялауға мүмкіндік береді. Таңдаулы орнату, Kaspersky бағдарламаларын басқару плагиндерінің қайсысы орнатылатынын көрсетуге мүмкіндік береді. Таңдаулы орнату кезінде, сіз тиісті параметрді көрсете отырып, ұялы құрылғыларға арналған орнату пакеттерін жасай аласыз.

3-қадам. Орнату үшін құрамдастарды таңдау

Орнатқыңыз келетін Kaspersky Security Center Басқару серверінің құрамдастарын таңдаңыз:

- **Ұялы құрылғыларды басқару**. Kaspersky Security Center орнату шебері жұмыс істеп тұрған кезде ұялы құрылғыларға орнату пакеттерін жасау қажет болса, осы жалаушаны қойыңыз. Сондай-ақ, Басқару серверін Басқару консолінің құралдарымен орнатқаннан кейін, ұялы құрылғыларға арналған орнату пакеттерін қолмен де жасауға болады.

- **SNMP агенті**. SNMP протоколы бойынша Басқару серверіне арналған статистикалық ақпаратты алады. Құрамдас, бағдарламаны SNMP құрамдасы орнатылған құрылғыға орнату кезде қолжетімді.

  > Kaspersky Security Center орнатылғаннан кейін, статистикалық ақпарат алу үшін қажетті mib файлдары салынған SNMP қалтасындағы бағдарламаны орнату қалтасында орналасады.

Желілік агент пен Басқару консолі құрамдастары құрамдастар тізімінде көрсетілмейді. Бұл құрамдастар автоматты түрде орнатылады, оларды орнатуды болдырмау мүмкін емес.

Шебердің осы қадамында да Басқару серверінің құрамдастарын орнату үшін қалтаны көрсетуі керек. Әдепкі бойынша, құрамдастар <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center қалтасына орнатылады. Осындай атауы бар қалта болмаса, ол орнату барысында автоматты түрде жасалады. Сіз мақсатты қалтаны **Шолу** түймесі арқылы өзгерте аласыз.

4-қадам. Kaspersky Security Center Web Console орнату

64 разрядты операциялық жүйені қолдансаңыз, бұл қадам көрсетілмейді. Әйтпесе, бұл қадам көрсетілмейді, өйткені Kaspersky Security Center Web Console веб-консолі 32 разрядты операциялық жүйелермен жұмыс істемейді.

Әдепкі бойынша, Kaspersky Security Center Web Console және Microsoft Management Console (MMC) негізіндегі Басқару консолі орнатылады.

Kaspersky Security Center Web Console веб-консолін ғана орнатқыңыз келсе:

1. **Консольдердің бірін орнату тармағын** таңдаңыз.
2. Ашылмалы тізімнен **Интернетке негізделген консоль** тармағын таңдаңыз.

Kaspersky Security Center Web Console орнату, Басқару серверін орнату аяқталғаннан кейін автоматты түрде іске қосылады.

Microsoft Management Console (MMC) негізінде Басқару консолін ғана орнатқыңыз келсе:

1. **Консольдердің бірін орнату тармағын** таңдаңыз.
2. Ашылмалы тізімнен **MMC негізіндегі консоль** тармағын таңдаңыз.

5-қадам. Желінің өлшемін таңдау

Kaspersky Security Center орнатылатын желінің өлшемін көрсетіңіз. Желідегі құрылғылардың санына байланысты, шебер орнату параметрлерін және бағдарлама интерфейсін көрсетуді конфигурациялайды.

Төмендегі кестеде желінің әртүрлі өлшемдерін таңдаған кезде бағдарламаны орнату және интерфейсті көрсету параметрлері атап көрсетілген.

Параметрлер	1–100 басқарылатын құрылғы	101–1000 басқарылатын құрылғы	1001–5000 басқарылатын құрылғы	5000-нан астам басқарылатын құрылғы
Қосалқы және виртуалды басқару серверлері және консоль тармағындағы қосалқы және виртуалды басқару серверлеріне қатысты барлық параметр үшін түйінмен көрсету (MMC негізіндегі басқару консольдерінде ғана қолжетімді)	Жоқ	Жоқ	Бар	Бар
Басқару серверінің және басқару топтарының сипаттар терезелеріндегі **Қауіпсіздік** бөлімдерімен көрсету (тек MMC негізіндегі басқару консолінде қолжетімді)	Жоқ	Жоқ	Бар	Бар
Клиент құрылғыларында жаңарту тапсырмасын іске қосу уақытын кездейсоқ бөлу	Жоқ	5 минуттық аралықта	10 минуттық аралықта	10 минуттық аралықта

Басқару серверін MySQL 5.7 және SQL Express дерекқор серверіне қосқан кезде 10 000-нан астам құрылғыны басқаруға арналған бағдарламаны пайдалану ұсынылмайды. MariaDB дерекқорларын басқару жүйесі үшін басқарылатын құрылғылардың ең көп ұсынылатын саны 20 000 құрайды.

6-қадам. Дерекқорды таңдау

Шебердің осы қадамында Басқару сервері дерекқорын сақтау үшін пайдаланылатын келесі дерекқорды басқару жүйелерінің (ДҚБЖ) бірін таңдаңыз:

- **Microsoft SQL сервері немесе SQL Server Express**
- **MySQL немесе MariaDB**
- **PostgreSQL немесе Postgres Pro**

Басқару серверін домен контроллеріне емес, бөлектенген серверге орнату ұсынылады. Тек оқуға арналған домен контроллері (RODC) рөлін атқаратын серверге Kaspersky Security Center орнатсаңыз, Microsoft SQL Server (SQL Express) жергілікті түрде орнатылмауы керек (дәл сол құрылғыда). Бұл жағдайда, Microsoft SQL Server (SQL Express) серверін қашықтан (басқа құрылғыға) орнату немесе ДҚБЖ жүйесін жергілікті түрде орнату қажет болса – MySQL, MariaDB не PostgreSQL пайдалану ұсынылады.

Басқару сервері дерекқорының құрылымы Kaspersky Security Center орнату қалтасында орналасқан klakdb.chm файлында келтірілген. Бұл файл Kaspersky порталындағы келесі мұрағатта да қолжетімді: klakdb.zip.

7-қадам. SQL сервері параметрлерін конфигурациялау

Шебердің осы қадамында, өзіңіз таңдаған дерекқорды басқару жүйесіне (ДҚБЖ) байланысты, келесі қосылым параметрлерін көрсетіңіз:

- Алдыңғы қадамда **Microsoft SQL сервері немесе SQL Server Express** таңдалған болсаңыз:
  - **SQL сервері үлгісінің атауы** өрісінде, желіде орнатылған SQL серверінің атауын көрсетіңіз. **Шолу** түймесінің көмегімен, желіде орнатылған барлық SQL серверлерінің тізімін аша аласыз. Әдепкі бойынша, өріс толтырылмаған.

SQL Server серверіне пайдаланушы порты арқылы қосылсаңыз, онда SQL Server данасының атауымен бірге порт нөмірін үтір арқылы көрсетіңіз, мысалы:

```
SQL_Server_host_name,1433
```

Басқару сервері мен SQL Server сервері арасындағы байланысты сертификат арқылы қорғасаңыз, **SQL сервері үлгісінің атауы** өрісінде сертификат жасау кезінде қолданылған дананың атауын көрсетіңіз. Аталған SQL Server данасын қолдансаңыз, SQL Server данасының атауымен бірге порт нөмірін үтір арқылы көрсетіңіз, мысалы:

```
SQL_Server_name,1433
```

Бір құрылғыда бірнеше SQL Server данасын қолдансаңыз, кері қиғаш сызық арқылы дананың атауын қосымша түрде көрсетіңіз, мысалы:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Корпоративтік желідегі SQL Server үшін Always On функциясы қосулы болса, **SQL сервері үлгісінің атауы** өрісінде қолжетімділік тобының тыңдаушысының атын енгізіңіз. Назар аударыңыз, Always On функциясы қосулы болған кезде Басқару сервері синхронды түрде бекітумен бірге қолжетімділік режимін ғана қолдайды.

- **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

Осы қадамда Kaspersky Security Center орнатып жатқан құрылғыға SQL серверін орнатқыңыз келсе, орнатуды доғарып, SQL серверін орнатқаннан кейін қайта іске қосуыңыз керек. Қолдау көрсетілетін SQL серверлері жүйеге қойылатын талаптарда көрсетілген.

SQL серверін қашықтағы құрылғыға орнатқыңыз келсе, Kaspersky Security Center орнату шеберінің жұмысын тоқтатудың қажеті жоқ. SQL Server серверін орнатыңыз және Kaspersky Security Center орнатуға оралыңыз.

- Алдыңғы қадамда **MySQL немесе MariaDB** таңдалған болсаңыз:
  - **SQL сервері үлгісінің атауы** өрісінде ДҚБЖ үлгінің атауын көрсетіңіз. Әдепкі бойынша, Kaspersky Security Center орнатылатын құрылғының IP мекенжайы қолданылады.
  - **Порт** өрісінде Басқару серверін DBMS серверінің дерекқорына қосу үшін портты көрсетіңіз. Әдепкі бойынша 3306-порт орнатылған.
  - **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.
- Алдыңғы қадамда **PostgreSQL немесе Postgres Pro** таңдалған болсаңыз:
  - **PostgreSQL немесе Postgres Pro сервері** өрісінде ДҚБЖ үлгінің атауын көрсетіңіз. Әдепкі бойынша, Kaspersky Security Center орнатылатын құрылғының IP мекенжайы қолданылады.
  - **Порт** өрісінде Басқару серверін ДҚБЖ-не қосу үшін портты көрсетіңіз. Әдепкі бойынша 5432-порт орнатылған.
  - **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

8-қадам. Түпнұсқалық растама режимін таңдау

Басқару серверін дерекқорларды басқару жүйесіне (ДҚБЖ) қосу кезінде қолданылатын түпнұсқалық растама режимін анықтаңыз.

Таңдалған ДҚБЖ жүйеге байланысты, сіз келесі түпнұсқалық растама режимдерін таңдай аласыз:

- SQL Express немесе Microsoft SQL Server үшін келесі нұсқалардың бірін таңдаңыз:

  - **Microsoft Windows аутентификация режимі**. Бұл жағдайда, құқықтарды тексеру кезінде Басқару серверін іске қосу үшін есептік жазба пайдаланылады.

  - **SQL серверінің аутентификация режимі**. Бұл нұсқа таңдалған жағдайда, құқықтарды тексеру үшін терезеде көрсетілген есептік жазба пайдаланылады. **Есептік жазба** және **Құпиясөз** өрістерін толтырыңыз.

    Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

  Бағдарлама дерекқордың екі түпнұсқалық растама режимі үшін қолжетімді ме екендігін тексереді. Дерекқор қолжетімді болмаса, қате туралы хабар пайда болады және сіз дұрыс есептік деректерді көрсетуіңіз қажет.

  > Басқару серверінің дерекқоры басқа құрылғыда болса және Басқару серверінің есептік жазбасы дерекқордың серверіне қатынаса алмаса, онда Басқару серверін орнату немесе жаңарту кезінде SQL серверінің түпнұсқалық растамасы режимін қолданған жөн. Бұл, дерекқоры бар құрылғы доменде болмаған кезде немесе Басқару сервері LocalSystem есептік жазбасымен орнатылған жағдайда орын алуы мүмкін.

- MySQL, MariaDB, PostgreSQL немесе Postgres Pro үшін есептік жазба мен құпиясөзді көрсетіңіз.

9-қадам. Басқару серверін іске қосу үшін есептік жазбаны таңдау

Басқару сервері қызмет ретінде іске қосылатын есептік жазбаны таңдаңыз.

- **Есептік жазбаны автоматты түрде жасау**. Бағдарлама, Басқару серверінің kladminserver қызметі іске қосылатын жергілікті KL-AK-* есептік жазбасын жасайды.

  Ортақ қатынасы бар қалтаны және ДҚБЖ жүйесін Басқару серверімен бір құрылғыға орналастыруды жоспарласаңыз, осы нұсқаны таңдай аласыз.

- **Есептік жазбаны таңдау**. Басқару сервері қызметі (kladminserver) сіз таңдаған есептік жазбамен іске қосылады.

  Мысалы, кез келген шығарылымдағы SQL серверін, соның ішінде басқа құрылғыда орналасқан SQL-express серверін ДҚБЖ ретінде пайдалануды жоспарласаңыз және/немесе ортақ қатынасы бар қалтаны басқа құрылғыда орналастыруды жоспарласаңыз, домендік есептік жазбаны таңдауыңыз қажет болады.

  Kaspersky Security Center бағдарламасы қызметтің басқарылатын есептік жазбаларын (MSA) және қызметтің топтық басқарылатын есептік жазбаларын (gMSA) қолдайды. Доменіңізде осындай есептік жазбалар қолданылса, олардың біреуін Басқару сервері қызметі үшін есептік жазба ретінде таңдай аласыз.

  MSA немесе gMSA таңдамас бұрын, есептік жазбаны Басқару серверін орнатқыңыз келетін құрылғыға орнатуыңыз керек. Есептік жазба әлі орнатылмаған болса, Басқару серверін орнатуды болдырмасаңыз, есептік жазбаны орнатыңыз және Басқару серверін орнатуды қайта іске қосыңыз. Жергілікті құрылғыда қызметтердің басқарылатын есептік жазбаларын орнату туралы қосымша ақпаратты Microsoft ресми құжаттамасынан қараңыз.

  MSA немесе gMSA көрсету үшін:

  1. **Шолу** түймесін басыңыз.

  2. Пайда болған терезеде **Нысан түрі** түймесін басыңыз.

3. **Қызметтерге арналған есептік жазба** түрін таңдап, **OK** түймесін басыңыз.

4. Қажетті есептік жазбаны таңдап, **OK** түймесін басыңыз.

Сіз таңдаған есептік жазба, қандай ДҚБЖ жүйесін қолдануды жоспарлап жатқаныңызға байланысты әртүрлі құқықтарға ие болуы тиіс.

Қауіпсіздік мақсатында, Басқару сервері іске қосылатын есептік жазбаға артықшылық бермеңіз.

Басқару сервері есептік жазбасын кейін өзгерту мүмкін емес. Басқару серверінің басқа есептік жазбасын пайдалану үшін failover кластерін қайта орнатуыңыз қажет.

10-қадам. Kaspersky Security Center қызметтерін іске қосу үшін есептік жазбаны таңдау

Осы құрылғыда Kaspersky Security Center қызметтері іске қосылатын есептік жазбаны таңдаңыз:

- **Есептік жазбаны автоматты түрде жасау**. Kaspersky Security Center бағдарламасы осы құрылғында kladmins тобында KlScSvc жергілікті есептік жазбасын жасайды. Kaspersky Security Center қызметтері жасалған есептік жазбамен іске қосылатын болады.

- **Есептік жазбаны таңдау**. Kaspersky Security Center қызметтері сіз таңдаған есептік жазбамен іске қосылатын болады.

  Сізге домендік есептік жазбаны таңдау, мысалы, басқа құрылғыда орналасқан қалтада есептерді сақтауды жоспарлап жатсаңыз немесе мұны ұйымыңыздың қауіпсіздік саясаты талап етіп жатса қажет болады. Сонымен қатар, сізге Басқару серверін істен шығуға төзімді кластерге орнату кезінде домендік есептік жазбаны таңдау қажет болуы мүмкін.

Қауіпсіздік мақсатында, қызметтер іске қосылатын есептік жазбаны артықшылықты етпеңіз.

Таңдалған есептік жазбаның астында KSN прокси-сервері (ksnproxy), Kaspersky белсендіру прокси-сервері (klactprx) және Kaspersky белсендіру порталы (klwebsrv) қызметтері іске қосылатын болады.

11-қадам. Ортақ қатынасы бар қалтаны анықтау

Келесі мақсаттар үшін пайдаланылатын ортақ қатынасы бар қалтаның орналасатын жерін және атауын анықтаңыз:

- бағдарламаларды қашықтан орнату үшін қажетті файлдарды сақтау (орнату пакеттерін жасау кезінде файлдар Басқару серверіне көшіріледі);

- жаңарту көзінен Басқару серверіне көшірілетін жаңартуларды орналастыру.

Бұл ресурсқа барлық пайдаланушылар үшін оқуға ортақ қатынасу құқығы ашылады.

Сіз келесі екі нұсқаның бірін таңдай аласыз:

- **Ортақ қатынас бар қалтаны жасау**. Жаңа қалта жасау. Төменде көрсетілген өрістегі қалтаға апаратын жолды көрсетіңіз.

- **Бұрыннан бар ортақ қалтаны таңдау**. Қолданыстағы қалталар ішінен ортақ қатынасы бар қалтаны таңдау.

Ортақ қатынасы бар қалта, орнату жүзеге асырылатын құрылғыда жергілікті түрде, сондай-ақ ұйым желісінің құрамына кіретін клиент құрылғыларының кез келгенінде қашықтан орналастырылуы мүмкін. Ортақ қатынасы бар қалтаны **Шолу** түймесінің көмегімен немесе тиісті өрісте UNC жолын енгізу арқылы қолмен (мысалы, \\server\Share) көрсете аласыз.

Әдепкісінше орнату бағдарламасы Kaspersky Security Center құрамдастарын қамтитын қолданба қалтасында жергілікті KLSHARE ішкі қалтасын жасайды.

Қажет болса, ортақ қатынасы бар қалтаны кейінірек анықтауға болады.

12-қадам. Басқару серверіне қосылу параметрлерін конфигурациялау

Басқару серверіне қосылу параметрлерін конфигурациялаңыз:

- **Порт**

  Басқару серверіне қосылу орындалатын порт нөмірі.

  Әдепкі бойынша 14000-порт орнатылған.

- **SSL порты**

  SSL протоколын қолдана отырып, Басқару серверіне қауіпсіз қосылу жүзеге асырылатын SSL порты нөмірі.

  Әдепкі бойынша 13000-порт орнатылған.

- **Шифрлау кілтінің ұзындығы**

  Шифрлау кілтінің ұзындығын таңдаңыз: 1024 бит немесе 2048 бит.

  1024 биттік ұзындығы бар шифрлау кілті процессорға аз жүктеме түсіреді, бірақ ескірген болып саналады және техникалық сипаттамалары жағынан сенімді түрде шифрлауды қамтамасыз ете алмауы мүмкін. Сондай-ақ, қолданыстағы жабдық 1024 биттік кілт ұзындығы бар SSL сертификаттарымен үйлесімді болмауы мүмкін.

  2048 биттік ұзындығы бар шифрлау кілті заманға сай шифрлау стандарттарына сай келеді. Дегенмен, 2048 биттік шифрлау кілтін пайдалану процессорға қосымша жүктеме түсіруі мүмкін.

  Әдепкі бойынша **2048 бит (жоғары қауіпсіздік)** нұсқасы таңдалған.

Басқару серверіне қосылу параметрлерін кейінірек өзгертуге болады:

- Сізге порт пен SSL порт нөмірлерін Басқару сервері сипаттарындағы **Қосылу порттары** бөлімінде өзгертуге болады. Басқару серверіне қосылу порттары туралы қосымша ақпаратты Kaspersky Security Center пайдаланатын порттар бөлімінен қараңыз.

- Басқару сервері сертификатын klsetsrvcert утилитасымен ауыстырған кезде шифрлау кілтінің ұзындығын `-o RsaKeyLen:<кілт ұзындығы>` параметрі арқылы өзгертуге болады.

13-қадам. Басқару сервері мекенжайын белгілеу

Басқару сервері мекенжайын келесі тәсілдердің бірімен көрсетіңіз:

- **DNS домені аты**. Бұл тәсіл, желіде DNS сервері болған кезде және клиент құрылғылары оның көмегімен Басқару серверінің мекенжайын ала алатын жағдайда қолданылады.
- **NetBIOS атауы**. Бұл тәсіл, клиент құрылғылары NetBIOS протоколы арқылы Басқару сервері мекенжайын алса немесе желіде WINS сервері болса қолданылады.
- **IP мекенжайы**. Бұл тәсіл, Басқару серверінде болашақта өзгермейтін статикалық IP мекенжайы болса қолданылады.

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің белсенді түйініне орнатып жатсаңыз және виртуалды желі адаптерін жасасаңыз, кластар түйіндерін дайындау кезінде осы адаптердің IP мекенжайын көрсетіңіз. Не болмаса, өзіңіз пайдаланып жатқан үшінші тарап теңгергішінің IP мекенжайын енгізіңіз.

14-қадам. Ұялы құрылғыларды қосу үшін Сервер мекенжайы

Орнату шеберінің бұл қадамы Ұялы құрылғыларды басқару құрамдасын орнатуды таңдаған кезде қолжетімді.

Ұялы құрылғыларды қосу мекенжайы терезесінде, жергілікті желіден тыс ұялы құрылғыларды қосу үшін Басқару серверінің сыртқы мекенжайын көрсетіңіз. Басқару серверінің IP мекенжайын немесе DNS (Domain Name System) мекенжайын көрсетуге болады.

15-қадам. Бағдарламаларды басқару плагиндерін таңдау

Kaspersky Security Center-мен бірге орнатылатын Kaspersky бағдарламаларын басқару плагиндерін таңдаңыз.

Оңай іздеу үшін плагиндер қорғалатын нысандардың түріне қарай топтарға бөлінеді.

16-қадам. Файлдарды мұрағаттан шығарып, қатты дискіге орнату

Kaspersky Security Center құрамдастарын орнату параметрлерін конфигурациялап болғаннан кейін, файлдарды қатты дискіге орнатуды іске қосуға болады.

Орнатуды іске қосу үшін қосымша бағдарламалар қажет болса, орнату шебері **Міндетті құрамдастарды орнату** терезесінде Kaspersky Security Center орнатуды бастамас бұрын хабарлайды. Қажетті бағдарламалар **Келесі** түймесін басқаннан кейін автоматты түрде орнатылады.

Соңғы бетте Kaspersky Security Center-мен жұмыс істеу үшін қандай консольді іске қосу керектігін таңдауға болады:

- **MMC негізіндегі Басқару консолін іске қосу**
- **Kaspersky Security Center Web Console консолін іске қосу**

  Бұл параметр, алдыңғы қадамдардың бірінде Kaspersky Security Center Web Console орнатуды таңдаған жағдайда ғана қолжетімді.

Сондай-ақ Kaspersky Security Center-мен жұмысты бастамай-ақ шеберді жабу үшін **Аяқтау** түймесін басуға болады. Kaspersky Security Center-мен жұмысты кейінірек кез келген уақытта бастауға болады.

Басқару консолін немесе Kaspersky Security Center Web Console веб-консолін бірінші рет іске қосу кезінде, бағдарламаны алғашқы рет конфигурациялай аласыз.

Ақауларға төзімді Kaspersky Security Center кластерін орналастыру

Бұл бөлімде ақауларға төзімді Kaspersky Security Center кластері туралы жалпы ақпарат, сондай-ақ ақауларға төзімді Kaspersky Security Center кластерін дайындау және желіде орналастыру нұсқаулары берілген.

Сценарий: Kaspersky Security Center ақауларға төзімді кластерін орналастыру

Ақауларға төзімді Kaspersky Security Center кластері Kaspersky Security Center бағдарламасының жоғары қолжетімділігін қамтамасыз етеді және апат болған жағдайда басқару серверінің босқа тұрып қалуын азайтады. Ақауларға төзімді кластер екі компьютерде орнатылған екі бірдей Kaspersky Security Center данасына негізделген. Даналардың бірі белсенді түйін ретінде, екіншісі пассивті түйін ретінде жұмыс істейді. Белсенді түйін клиент құрылғыларын қорғауды басқарады, ал пассивті белсенді түйін істен шыққан жағдайда – белсенді түйіннің барлық функцияларын қабылдауға дайын. Апат болған кезде пассивті түйін белсенді болады, ал белсенді түйін пассивті болады.

Алдын ала талаптар

Сізде ақауларға төзімді кластер талаптарына сәйкес келетін жабдық бар.

Кезеңдер

Kaspersky бағдарламалық жасақтамасын орналастыру келесі кезеңдерден тұрады:

1. **Kaspersky Security Center қызметтері үшін есептік жазба жасау**

   Домендік топ құрыңыз (бұл сценарийде топ үшін "KLAdmins" атауы қолданылады) және жергілікті әкімші құқықтарын екі түйінде де, файл серверінде де топқа беріңіз. Содан кейін, домен пайдаланушыларының екі есептік жазбасын жасаңыз (бұл сценарийде осы есептік жазбалар үшін "ksc" және "rightless" атаулары қолданылады) және KLAdmins домендік тобына есептік жазбаларды қосыңыз.

   Бұрын жасалған KLAdmins домендік тобына Kaspersky Security Center орнатылатын пайдаланушы есептік жазбасын қосыңыз.

2. **Файл серверін дайындау**

   Файл серверін ақауларға төзімді Kaspersky Security Center кластерінің құрамында жұмыс істеуге дайындаңыз. Файл сервері аппараттық және бағдарламалық жасақтама талаптарына сәйкес келетініне көз жеткізіңіз, Kaspersky Security Center деректері үшін екі ортақ қатынасы бар қалта жасаңыз және ортақ қатынасы бар қалталарға қатынасу құқықтарын конфигурациялаңыз.

   Нұсқаулар: ақауларға төзімді Kaspersky Security Center кластері үшін файлдық серверді дайындау

3. **Белсенді және пассивті түйіндерді дайындау**

   Белсенді және белсенді емес түйіндер ретінде жұмыс істеу үшін бірдей аппараттық және бағдарламалық жасақтамасы бар екі құрылғыны дайындаңыз.

   Нұсқаулар: ақауларға төзімді Kaspersky Security Center кластері үшін түйіндерді дайындау

4. **Дерекқорды басқару жүйесін (ДҚБЖ) орнату**

   Қолдау көрсетілетін кез келген ДҚБЖ таңдаңыз және ДҚБЖ-ны арнайы құрылғыға орнатыңыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында берілген.

5. **Kaspersky Security Center орнату**

   Kaspersky Security Center бағдарламасын істен шығуға төзімді кластер режимінде екі түйінге де орнатыңыз. Алдымен Kaspersky Security Center бағдарламасын белсенді хост болатын құрылғыға, содан кейін енжар хостқа орнату керек.

   Сондай-ақ Kaspersky Security Center Web Console веб-консолін кластер түйіні емес бөлек құрылғыға орнатуыңыз керек.

   Нұсқаулар: Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйіндеріне орнату

6. **Істен шығуға төзімді кластерді тестілеу**

   Істен шығуға төзімді кластерді дұрыс конфигурациялағаныңызға және оның дұрыс жұмыс істеп тұрғанына көз жеткізіңіз. Мысалы, сіз Kaspersky Security Center қызметтерінің бірін белсенді түйінде тоқтата аласыз: kladminserver, klnagent, ksnproxy, klactprx немесе klwebsrv. Қызмет тоқтағаннан кейін, қорғауды басқару автоматты түрде пассивті түйінге ауысуы керек.

Нәтижелер

Ақауларға төзімді Kaspersky Security Center кластері орналастырылды. Белсенді және пассивті түйіндер арасында ауысуға әкелетін оқиғалармен танысып шығыңыз.

Ақауларға төзімді Kaspersky Security Center кластері туралы ақпарат

Ақауларға төзімді Kaspersky Security Center кластері Kaspersky Security Center бағдарламасының жоғары қолжетімділігін қамтамасыз етеді және апат болған жағдайда басқару серверінің босқа тұрып қалуын азайтады. Ақауларға төзімді кластер екі компьютерде орнатылған екі бірдей Kaspersky Security Center данасына негізделген. Даналардың бірі белсенді түйін ретінде, екіншісі пассивті түйін ретінде жұмыс істейді. Белсенді түйін клиент құрылғыларын қорғауды басқарады, ал пассивті белсенді түйін істен шыққан жағдайда – белсенді түйіннің барлық функцияларын қабылдауға дайын. Апат болған кезде пассивті түйін белсенді болады, ал белсенді түйін пассивті болады.

Ақауларға төзімді кластерді пайдалану Өлшеу нұсқаулығына негізделген есептерге әсер етпейді.

Ақауларды жою үшін Kaspersky Event журналы мүмкіндігін пайдаланыңыз.

Kaspersky Security Center географиялық таратылған орын басу кластеріне қолдау көрсетілмейді. Kaspersky Security Center ауыстырып қосу кластерін тек бір географиялық сайт ішінде орналастыруға болады.

Ауысу шарты

Істен шығуға төзімді кластер клиент құрылғыларын қорғауды басқаруды белсенді түйіннен пассивті түйінге ауыстырады, егер белсенді түйінде келесі оқиғалардың кез келгені орын алса:

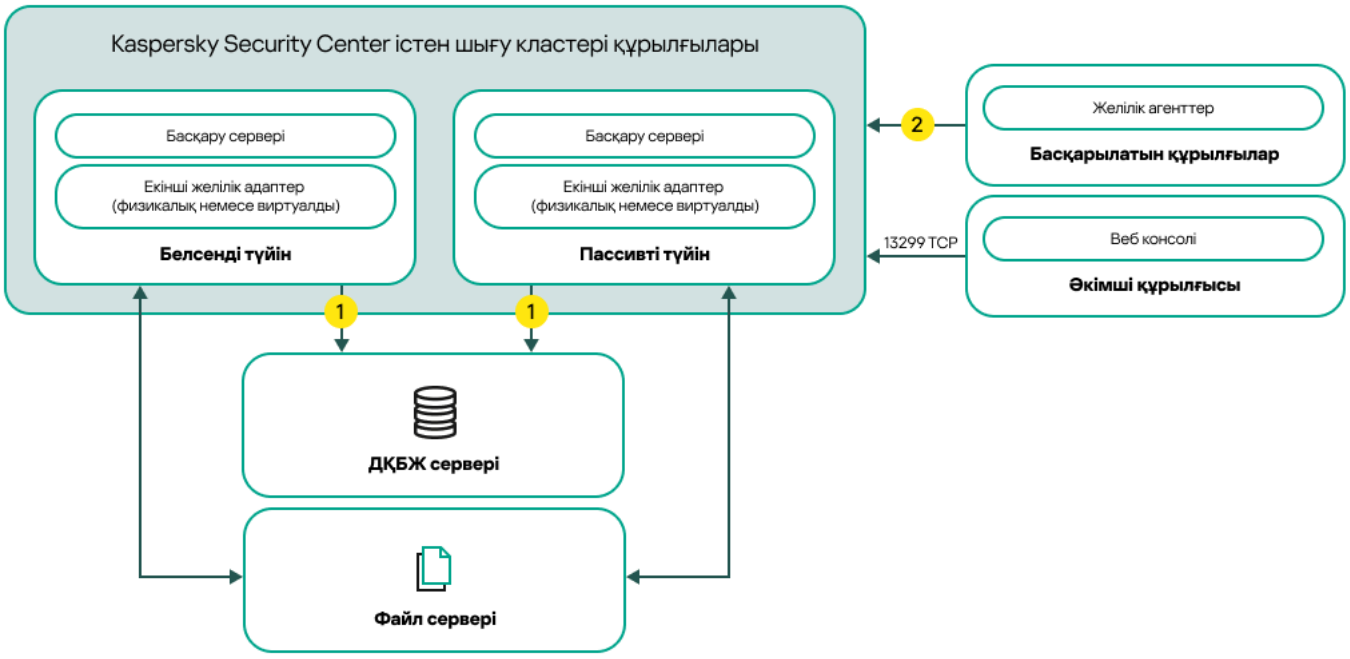
- Белсенді түйін бағдарламалық немесе аппараттық ақауға байланысты сынған.
- Техникалық жұмыстарды жүргізу үшін белсенді түйін уақытша тоқтатылды.
- Kaspersky Security Center қызметтерінің (немесе процестерінің) кем дегенде біреуі қатемен аяқталды немесе пайдаланушы оны әдейі тоқтатты. Kaspersky Security Center қызметтеріне мыналар жатады: kladminserver, klnagent, klactprx және klwebsrv.
- Белсенді түйін мен файл сервериндегі қойма арасындағы желілік қосылым доғарылды немесе үзілді.

Ақауларға төзімді Kaspersky Security Center кластері барлық Kaspersky Security Center қызметін автоматты түрде басқарады. Қызметтерді қолмен қайта іске қоспаңыз.

Орналастыру схемалары

Kaspersky Security Center ақауларға төзімді кластерін орналастыру үшін келесі схемалардың бірін таңдауға болады:

- Қосымша желілік адаптерді пайдаланатын схема.
- Үшінші тараптың жүктемені теңестіруін пайдаланатын схема.

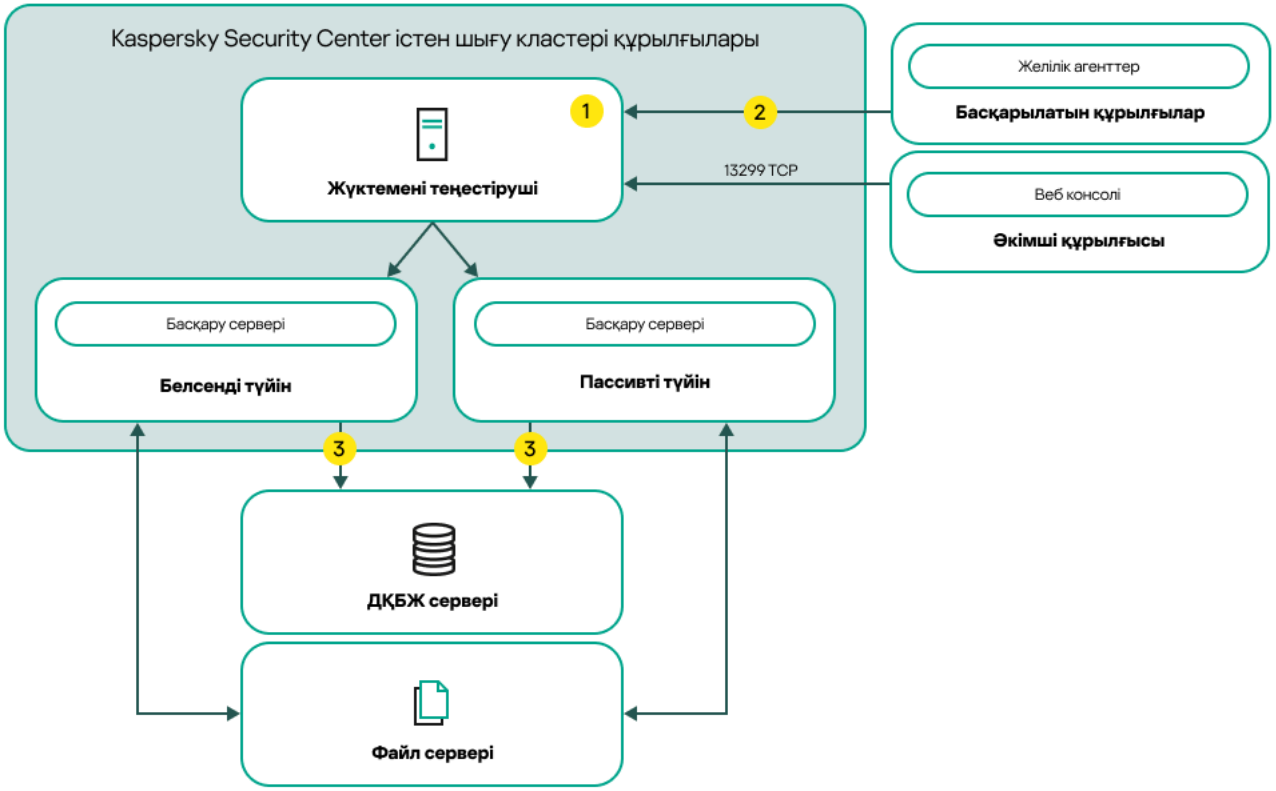


Қосымша желілік адаптерді пайдаланатын схема

Схеманың шартты белгілері:

1 Басқару сервері деректерді дерекқорға жібереді. MySQL сервері үшін 3306 порты немесе Microsoft SQL Server үшін 1433 порты сияқты дерекқор орналасқан құрылғыда қажетті порттарды ашыңыз. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

2 Басқарылатын құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.



Үшінші тараптың жүктемені теңестіруін пайдаланатын схема

Схеманың шартты белгілері:

1 Жүктемені теңдестіру құрылғысында барлық басқару сервері портын ашыңыз: TCP 13000, UDP 13000, TCP 13299 және TCP 17000.

> Автоматтандыру үшін klakaut утилитасын пайдаланғыңыз келсе, TCP 13291 портын да ашуыңыз керек.

2 Басқарылатын құрылғыларда келесі порттарды ашыңыз: TCP 13000, UDP 13000 және TCP 17000.

3 Басқару сервері деректерді дерекқорға жібереді. MySQL сервері үшін 3306 порты немесе Microsoft SQL Server үшін 1433 порты сияқты дерекқор орналасқан құрылғыда қажетті порттарды ашыңыз. Толығырақ ақпарат ДҚБЖ құжаттамасында көрсетілген.

Ақауларға төзімді Kaspersky Security Center кластері үшін файлдық серверді дайындау

Файлдық сервер ақауларға төзімді Kaspersky Security Center кластерінің міндетті құрамдасы сияқты жұмыс істейді.

Файл серверін дайындау үшін:

1. Файл сервері аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз.
2. Файл сервері мен екі түйіннің (белсенді және пассивті) бір доменге қосылғанына немесе файл сервері домен контроллері болып табылатынына көз жеткізіңіз.

3. Файл серверінде екі ортақ қатынасы бар қалта жасаңыз. Олардың бірі істен шығуға төзімді кластердің күйі туралы ақпаратты сақтау үшін қолданылады. Екіншісі Kaspersky Security Center деректері мен параметрлерін сақтау үшін қолданылады. Kaspersky Security Center орнату кезінде ортақ қатынасы бар қалталарға жолдарды көрсету керек.

4. Келесі пайдаланушы есептік жазбалары мен топтары үшін жасалған ортақ қатынасы бар қалталарға толық қатынасу құқықтарын (ортақ қатынасу құқықтары да, NTFS рұқсаттары да) беріңіз:

   - KLAdmins домендік тобы.

   - Пайдаланушылардың $<node1> және $<node2> есептік жазбалары. Мұндағы <node1> және <node2> — белсенді және белсенді емес түйіндердің құрылғы атаулары.

Файл сервері дайындалды. Ақауларға төзімді Kaspersky Security Center кластерін орналастыру үшін осы сценарий нұсқауларын орындаңыз.

Ақауларға төзімді Kaspersky Security Center кластері үшін түйіндерді дайындау

Екі құрылғыны Kaspersky Security Center ақауларға төзімді кластері үшін белсенді және белсенді емес түйін ретінде жұмыс істеуге дайындаңыз.

Ақауларға төзімді Kaspersky Security Center кластеріне түйіндерді дайындау үшін:

1. Аппараттық және бағдарламалық талаптарға сәйкес келетін екі құрылғыңыз бар екеніне көз жеткізіңіз. Бұл құрылғылар ақауларға төзімді кластердің белсенді және белсенді емес түйіндері ретінде әрекет етеді.

2. Файл сервері мен екі түйіннің бір доменге қосылғанына көз жеткізіңіз.

3. Келесі әрекеттердің бірін орындаңыз:

   - Түйіндердің әрқайсысында қосымша желілік адаптерді конфигурациялаңыз.

     Қосымша желілік адаптер физикалық немесе виртуалды болуы мүмкін. Физикалық желілік адаптерді пайдаланғыңыз келсе, оны стандартты операциялық жүйе құралдары арқылы қосыңыз және конфигурациялаңыз. Виртуалды желілік адаптерді пайдаланғыңыз келсе, оны үшінші тарап бағдарламалары арқылы жасаңыз

     Келесі шарттардың орындалғанына көз жеткізіңіз:

     - Қосымша желілік адаптерлер өшірілген.

       Сіз қосымша желілік адаптерлерді ажыратылған күйде жасай аласыз немесе оларды жасағаннан кейін өшіре аласыз.

     - Екі түйіндегі қосымша желілік адаптерлерде бірдей IP мекенжайы болуы керек.

   - Үшінші тарап жүктеме теңестіргішін пайдаланыңыз. Мысалы, nginx серверін пайдалануға болады. Бұл жағдайда келесі әрекеттерді орындаңыз:

     a. nginx орнатылған Linux негізіндегі арнайы құрылғыны ұсыныңыз.

     b. Жүктемені теңестіруді конфигурациялаңыз. Негізгі сервер ретінде белсенді түйінді және резервтік сервер ретінде пассивті түйінді орнатыңыз.

c. nginx серверінде барлық басқару сервері портын ашыңыз: TCP 13000, UDP 13000, TCP 13299 және TCP 17000.

> Автоматтандыру үшін klakaut утилитасын пайдаланғыңыз келсе, TCP 13291 портын да ашуыңыз керек.

4. Екі түйінді және файл серверін қайта іске қосыңыз.

5. Файл серверін дайындау кезеңінде жасаған екі ортақ қатынасы бар қалтаны түйіндердің әрқайсысына сәйкестендіріңіз. Ортақ қатынасы бар қалталарды желілік дискілер ретінде салыстыруыңыз керек. Қалталарды салыстыру кезінде кез келген бос диск әріптерін таңдауға болады. Ортақ қатынасы бар қалталарға қатынасу үшін сценарийдің 1-қадамында жасаған пайдаланушы есептік жазбасының есептік деректерін пайдаланыңыз.

Түйіндер дайындалды. Ақауларға төзімді Kaspersky Security Center кластерін орналастыру үшін сценарий нұсқауларын орындаңыз.

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйіндеріне орнату

Kaspersky Security Center бағдарламасы ақауларға төзімді Kaspersky Security Center кластерінің екі түйініне жеке-жеке орнатылады. Алдымен бағдарламаны белсенді түйінге, содан кейін пассивті түйінге орнатасыз. Орнату кезінде сіз қай түйіннің белсенді және қайсысы пассивті болатынын таңдайсыз.

> KLAdmins домендік тобының пайдаланушысы ғана әр түйінге Kaspersky Security Center бағдарламасын орната алады.

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің белсенді түйініне орнату үшін:

1. ksc_15.1.<жинақ нөмірі>_full_<локализация тілі>.exe орындалатын файлын іске қосыңыз.

   Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. **Kaspersky Security Center Басқару серверін орнату** сілтемесі бойынша бағдарламаларды таңдау терезесінде Басқару серверін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

2. Сіз бен Kaspersky арасында жасалатын Лицензиялық келісімді және Құпиялылық саясатын мұқият оқып шығыңыз. Лицензиялық келісім мен Құпиялық саясатының барлық тармақтарымен келіссеңіз, **Толығымен оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** блогында келесі жалаушаларды қойыңыз:

   - **Осы Лицензиялық келісімнің ережелері мен шарттары**
   - **Деректердің өңделуін сипаттайтын Құпиялылық саясаты**

   Бағдарламаны орнату келесі екі жалаушаны қойғаннан кейін жалғасады.

   Лицензиялық келісіммен немесе Құпиялылық саясатымен келіспесеңіз, **Бас тарту** түймесін басып, бағдарламаны орнатуды болдырмаңыз.

3. Бағдарламаны белсенді түйінге орнату үшін **Ақауларға төзімді Kaspersky Security Center кластерінің негізгі түйіні** тармағын таңдаңыз.

4. **Ортақ қатынасы бар қалта** терезесінде келесі әрекетті орындаңыз:

   - **Мемлекеттік үлес** және **Деректер үлесі** өрістерінде, дайындық барысында файл серверінде жасалған ортақ қатынасы бар қалталарға апаратын жолды көрсетіңіз.
   - **Мемлекеттік үлес жетегі** және **Деректер үлесінің жетегі** өрістерінде түйіндерді дайындау барысында ортақ қатынасы бар қалталар қосылған желілік дискілерді таңдаңыз.
   - Кластердің қосылым режимін таңдаңыз: қосымша желілік адаптер немесе үшінші тарап жүктеме теңгергіші арқылы.

5. Таңдаулы орнатудың басқа қадамдарын 3-қадамнан бастап орындаңыз.

> 13-қадамда, адаптер жасаған болсаңыз, кластер түйіндерін дайындау барысында қосымша желілік адаптердің IP мекенжайын көрсетіңіз. Не болмаса, өзіңіз пайдаланып жатқан үшінші тарап теңгергішінің IP мекенжайын енгізіңіз.

Kaspersky Security Center бағдарламасы белсенді түйінге орнатылған.

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің пассивті түйініне орнату үшін:

1. ksc_15.1.<жинақ нөмірі>_full_<локализация тілі>.exe орындалатын файлын іске қосыңыз.

   Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. **Kaspersky Security Center Басқару серверін орнату** сілтемесі бойынша бағдарламаларды таңдау терезесінде Басқару серверін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

2. Сіз бен Kaspersky арасында жасалатын Лицензиялық келісімді және Құпиялылық саясатын мұқият оқып шығыңыз. Лицензиялық келісім мен Құпиялық саясатының барлық тармақтарымен келіссеңіз, **Толығымен оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** блогында келесі жалаушаларды қойыңыз:

   - **Осы Лицензиялық келісімнің ережелері мен шарттары**
   - **Деректердің өңделуін сипаттайтын Құпиялылық саясаты**

   Бағдарламаны орнату келесі екі жалаушаны қойғаннан кейін жалғасады.

   Лицензиялық келісіммен немесе Құпиялылық саясатымен келіспесеңіз, **Бас тарту** түймесін басып, бағдарламаны орнатуды болдырмаңыз.

3. Бағдарламаны пассивті түйінге орнату үшін **Ақауларға төзімді Kaspersky Security Center кластерінің қосалқы түйіні** тармағын таңдаңыз.

4. **Ортақ қатынасы бар қалта** терезесінде, **Мемлекеттік үлес** өрісінде, дайындықтан кейін файл серверінде жасалған кластер күйі туралы ақпараты бар ортақ қатынасы бар қалтаға апаратын жолды көрсетіңіз.

5. **Орнату** түймесін басыңыз. Орнату аяқталғаннан кейін, **Аяқтау** түймесін басыңыз.

Kaspersky Security Center бағдарламасы пассивті түйінге орнатылған. Енді сіз дұрыс конфигурациялағаныңызға және кластердің дұрыс жұмыс істеп тұрғанына көз жеткізу үшін ақауларға төзімді Kaspersky Security Center кластерін тексере аласыз.

Кластер түйінін қолмен іске қосу және тоқтату

Сізге ақауларға төзімді барлық Kaspersky Security Center кластерін тоқтату қажет болуы немесе қызмет көрсету үшін кластер түйіндерінің бірін уақытша өшіру қажет болуы мүмкін. Бұл жағдайда, осы бөлімдегі нұсқауларды орындаңыз. Басқа құралдардың көмегімен істен шығуға төзімді кластермен байланысты қызметтерді немесе процестерді істен шығуға немесе тоқтатуға тырыспаңыз. Бұл деректердің жоғалуына әкелуі мүмкін.

Қызмет көрсету үшін істен шығуға төзімді кластерді іске қосу және тоқтату

Барлық істен шығуға төзімді кластерді іске қосу немесе тоқтату үшін:

1. Белсенді түйінде <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center қалтасына өтіңіз.
2. Пәрмен жолын ашып, келесі пәрмендердің бірін орындаңыз:
   - Кластерді тоқтату үшін `klfoc -stopcluster --stp klfoc` пәрменін орындаңыз
   - Кластерді іске қосу үшін `klfoc -startcluster --stp klfoc` пәрменін орындаңыз

Істен шығуға төзімді кластер пәрменге байланысты іске қосылады немесе тоқтайды.

Түйіндердің біріне қызмет көрсету

Түйіндердің біріне қызмет көрсету үшін:

1. Істен шығуға төзімді түйінде `klfoc -stopcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді тоқтатыңыз.
2. Қызмет көрсеткіңіз келетін түйінде <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center қалтасына өтіңіз.
3. `detach_node.cmd` пәрменін орындау арқылы пәрмен жолын ашып, түйінді кластерден ажыратыңыз.
4. Істен шығуға төзімді түйінде `klfoc -startcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді іске қосыңыз.
5. Техникалық қызмет көрсету жұмыстарын орындаңыз.
6. Істен шығуға төзімді түйінде `klfoc -stopcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді тоқтатыңыз.
7. Қызмет көрсетілетін түйінде <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center қалтасына өтіңіз.

8. `attach_node.cmd` пәрменін орындау арқылы пәрмен жолын ашып, түйінді кластерге қосыңыз.

9. Істен шығуға төзімді түйінде `klfoc -startcluster --stp klfoc` пәрменінің көмегімен істен шығуға төзімді кластерді іске қосыңыз.

Түйінге қызмет көрсетіліп, ол істен шығуға төзімді кластерге қосылады.

Басқару серверін ақауларға төзімді Windows Server кластеріне орнату

Басқару серверін істен шығуға төзімді кластерге орнату процедурасы автономды құрылғыдағы стандартты және таңдаулы орнатудан ерекшеленеді.

> Windows географиялық таратылған ауыстырып қосу кластерлеуіне қолдау көрсетілмейді. Windows Server ақауларға төзімді кластерін өрістету тек желінің жоғары қолжетімділігі мен кластер түйіндері арасындағы жылдам жауап беру уақытын қамтамасыз ететін бір географиялық нысан шегінде ғана мүмкін болады.

Осы бөлімде, кластердің жалпы деректер қоймасын қамтитын түйінде сипатталған процедураны орындаңыз.

Кластерге Kaspersky Security Center Басқару серверін орнату үшін,

орындалатын ksc_<нұсқа нөмірі>.<жинақ нөмірі>_full_<локализация тілі>.exe файлын іске қосыңыз.

Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. **Kaspersky Security Center Басқару серверін орнату** сілтемесі бойынша бағдарламалар таңдалатын терезеде Басқару серверін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

1-қадам. Лицензиялық келісім мен Құпиялық саясатын қарап шығу

Орнату шеберінің осы қадамында, сіз бен Kaspersky арасында жасалатын Лицензиялық келісім және Құпиялылық саясатымен танысу қажет.

Сондай-ақ, сізден Kaspersky Security Center дистрибутивінде қолжетімді бағдарламаларды басқару плагиндеріне Лицензиялық келісімдермен және Құпиялылық саясаттарымен танысу сұралуы мүмкін.

Сіз бен Kaspersky арасында жасалатын Лицензиялық келісімді және Құпиялылық саясатын мұқият оқып шығыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шарттарымен келіссеңіз, мұны тиісті жалаушаларды белгілеу арқылы растаңыз.

Бағдарламаны орнату келесі екі жалаушаны қойғаннан кейін жалғасады.

Лицензиялық келісіммен немесе Құпиялылық саясатымен келіспесеңіз, **Бас тарту** түймесін басып, бағдарламаны орнатуды болдырмаңыз.

2-қадам. Кластерге орнату түрін таңдау

Кластерге орнату түрін таңдаңыз:

- **Кластер (кластердің барлық түйіндерінде орнату)**

  Осы параметрді таңдау ұсынылады. Осы параметрді таңдасаңыз, Басқару сервері кластердің барлық түйіндерінде бір уақытта орнатылады.

  > Орнату үшін Басқару консолін таңдау қадамында ағымдағы кластер түйінінде орнатылатын Консольді таңдау керек. Консольді тек кластер түйініне орнатсаңыз, түйін істен шықса, сіз Басқару серверіне қатынасу құқығын жоғалтасыз. Осы қадамда барлық кластер түйіндеріне орнату үшін Microsoft басқару консолі (MMC) негізіндегі Басқару консолін таңдауды ұсынамыз. Басқару серверін орнатқаннан кейін Kaspersky Security Center Web Console веб-консолін кластер түйіні болып табылмайтын бөлек құрылғыға орнатыңыз. Бұл кластер түйіні істен шыққан жағдайда Kaspersky Security Center Web Console веб-консолін пайдаланып, Басқару серверін басқаруға мүмкіндік береді.

- **Жергілікті түрде (тек осы құрылғыға ғана орнату)**

  Осы параметрді таңдасаңыз, Басқару сервері тек ағымдағы түйінде, автономды сервердегідей орнатылады және Басқару сервері кластерлік бағдарлама ретінде жұмыс істемейді. Мысалы, Басқару сервері үшін істен шығуға төзімділік қажет болмаса, осы параметрді жалпы қоймада бос кеңістікті үнемдеу үшін таңдай аласыз. Ағымдағы түйін істен шыққан жағдайда, сізге Басқару серверін басқа түйінге орнатып, деректердің сақтық көшірмесінен Басқару серверінің күйін қалпына келтіру тура келеді.

Кейінгі әрекеттер, орнату тәсілін таңдаудан бастап, стандартты немесе таңдаулы орнату тәсілін қолдану кезіндегідей болып келеді.

3-қадам. Виртуалды Басқару сервері атауын көрсету

Жаңа виртуалды Басқару серверінің желілік атауын көрсетіңіз. Сіз осы атауды Басқару консолін немесе Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу үшін қолдана аласыз.

Көрсетілген атау кластердің атауынан ерекшеленуі тиіс.

4-қадам. Виртуалды Басқару сервері желісінің параметрлерін көрсету

Виртуалды Басқару серверінің жаңа үлгісінің желілік деректерін көрсету үшін:

1. **Пайдаланылатын желі** бөлімінде кластердің ағымдағы түйіні қосылған домен желісін таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:
   - DHCP таңдалған желіде IP мекенжайларын тағайындау үшін қолданылса, онда **DHCP пайдалану** параметрін таңдаңыз.
   - DHCP таңдалған желіде қолданылмаса, онда қажетті IP мекенжайын көрсетіңіз.

     Сіз көрсеткен IP мекенжайы кластердің IP мекенжайынан ерекшеленуі тиіс.
3. Көрсетілген параметрлерді қолдану үшін **Қосу** түймесін басыңыз.

Сіз автоматты түрде тағайындалған немесе көрсетілген IP мекенжайын Басқару консолін немесе Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу үшін қолдана аласыз.

5-қадам. Кластерлер тобын көрсету

Кластер тобы – барлық түйіндер үшін ортақ ресурстарды қамтитын істен шығуға төзімді кластердің ерекше рөлі. Сіздің екі нұсқаңыз бар:

- Жаңа кластерлік топты жасау.

  Бұл нұсқа көптеген жағдайда ұсынылады. Жаңа кластер тобы Басқару серверінің үлгісіне қатысты барлық ортақ ресурстарды қамтитын болады.

- Бұрыннан бар кластерлер тобын таңдау.

  Бұрыннан бар кластер тобымен байланысты ортақ ресурстарды қолданғыңыз келсе, осы параметрді таңдаңыз. Мысалы, сіз бұрыннан бар кластер тобымен байланысты қойманы қолданғыңыз келсе және жаңа кластер тобы үшін басқа қолжетімді қойма болмаса, осы нұсқаны қолдана аласыз.

6-қадам. Кластерлік деректер қоймасын таңдау

Кластерлік деректер қоймасын таңдау үшін:

1. **Қолжетімді қоймалар** бөлімінде, виртуалды Басқару сервері үлгісінің ортақ ресурстары орнатылатын қойманы таңдаңыз.
2. Таңдалған деректер қоймасында бірнеше том болса, **Дискіде қолжетімді бөлімдер** бөлімінде қажетті томды таңдаңыз.
3. **Орнату жолы** өрісінде, виртуалды Басқару сервері үлгісінің ресурстары орнатылатын ортақ деректер қоймасына апаратын жолды енгізіңіз.

Деректер қоймасы таңдалды.

7-қадам. Қашықтан орнату үшін есептік жазбаны көрсету

Виртуалды Басқару серверінің үлгісін пассивті кластер түйініне қашықтан орнату үшін қолданылатын пайдаланушы аты мен құпиясөзін көрсетіңіз.

Сіз көрсеткен есептік жазба үшін кластердің барлық түйіндерінде әкімші құқықтары ұсынылуы тиіс.

8-қадам. Орнату үшін құрамдастарды таңдау

Орнатқыңыз келетін Kaspersky Security Center Басқару серверінің құрамдастарын таңдаңыз:

- **Ұялы құрылғыларды басқару**. Kaspersky Security Center орнату шебері жұмыс істеп тұрған кезде ұялы құрылғыларға орнату пакеттерін жасау қажет болса, осы жалаушаны қойыңыз. Сондай-ақ, Басқару серверін Басқару консолінің құралдарымен орнатқаннан кейін, ұялы құрылғыларға арналған орнату пакеттерін қолмен де жасауға болады.

- **SNMP агенті**. SNMP протоколы бойынша Басқару серверіне арналған статистикалық ақпаратты алады. Құрамдас, бағдарламаны SNMP құрамдасы орнатылған құрылғыға орнату кезде қолжетімді.

  > Kaspersky Security Center орнатылғаннан кейін, статистикалық ақпарат алу үшін қажетті mib файлдары салынған SNMP қалтасындағы бағдарламаны орнату қалтасында орналасады.

Желілік агент пен Басқару консолі құрамдастары құрамдастар тізімінде көрсетілмейді. Бұл құрамдастар автоматты түрде орнатылады, оларды орнатуды болдырмау мүмкін емес.

Шебердің осы қадамында да Басқару серверінің құрамдастарын орнату үшін қалтаны көрсетуі керек. Әдепкі бойынша, құрамдастар <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center қалтасына орнатылады. Осындай атауы бар қалта болмаса, ол орнату барысында автоматты түрде жасалады. Сіз мақсатты қалтаны **Шолу** түймесі арқылы өзгерте аласыз.

9-қадам. Желінің өлшемін таңдау

Kaspersky Security Center орнатылатын желінің өлшемін көрсетіңіз. Желідегі құрылғылардың санына байланысты, шебер орнату параметрлерін және бағдарлама интерфейсін көрсетуді конфигурациялайды.

Төмендегі кестеде желінің әртүрлі өлшемдерін таңдаған кезде бағдарламаны орнату және интерфейсті көрсету параметрлері атап көрсетілген.

Параметрлер	1–100 басқарылатын құрылғы	101–1000 басқарылатын құрылғы	1001–5000 басқарылатын құрылғы	5000-нан астам басқарылатын құрылғы
Қосалқы және виртуалды басқару серверлері және консоль тармағындағы қосалқы және виртуалды басқару серверлеріне қатысты барлық параметр үшін түйінмен көрсету (MMC негізіндегі басқару консольдерінде ғана қолжетімді)	Жоқ	Жоқ	Бар	Бар
Басқару серверінің және басқару топтарының сипаттар терезелеріндегі **Қауіпсіздік** бөлімдерімен көрсету (тек MMC негізіндегі басқару консолінде қолжетімді)	Жоқ	Жоқ	Бар	Бар
Клиент құрылғыларында жаңарту тапсырмасын іске қосу уақытын кездейсоқ бөлу	Жоқ	5 минуттық аралықта	10 минуттық аралықта	10 минуттық аралықта

Басқару серверін MySQL 5.7 және SQL Express дерекқор серверіне қосқан кезде 10 000-нан астам құрылғыны басқаруға арналған бағдарламаны пайдалану ұсынылмайды. MariaDB дерекқорларын басқару жүйесі үшін басқарылатын құрылғылардың ең көп ұсынылатын саны 20 000 құрайды.

10-қадам. Дерекқорды таңдау

Шебердің осы қадамында Басқару сервері дерекқорын сақтау үшін пайдаланылатын келесі дерекқорды басқару жүйелерінің (ДҚБЖ) бірін таңдаңыз:

- **Microsoft SQL сервері немесе SQL Server Express**
- **MySQL немесе MariaDB**
- **PostgreSQL немесе Postgres Pro**

Басқару серверін домен контроллеріне емес, бөлектенген серверге орнату ұсынылады. Тек оқуға арналған домен контроллері (RODC) рөлін атқаратын серверге Kaspersky Security Center орнатсаңыз, Microsoft SQL Server (SQL Express) жергілікті түрде орнатылмауы керек (дәл сол құрылғыда). Бұл жағдайда, Microsoft SQL Server (SQL Express) серверін қашықтан (басқа құрылғыға) орнату немесе ДҚБЖ жүйесін жергілікті түрде орнату қажет болса – MySQL, MariaDB не PostgreSQL пайдалану ұсынылады.

Басқару сервері дерекқорының құрылымы Kaspersky Security Center орнату қалтасында орналасқан klakdb.chm файлында келтірілген. Бұл файл Kaspersky порталындағы келесі мұрағатта да қолжетімді: klakdb.zip.

11-қадам. SQL сервері параметрлерін конфигурациялау

Шебердің осы қадамында, өзіңіз таңдаған дерекқорды басқару жүйесіне (ДҚБЖ) байланысты, келесі қосылым параметрлерін көрсетіңіз:

- Алдыңғы қадамда **Microsoft SQL сервері немесе SQL Server Express** таңдалған болсаңыз:
  - **SQL сервері үлгісінің атауы** өрісінде, желіде орнатылған SQL серверінің атауын көрсетіңіз. **Шолу** түймесінің көмегімен, желіде орнатылған барлық SQL серверлерінің тізімін аша аласыз. Әдепкі бойынша, өріс толтырылмаған.

SQL Server серверіне пайдаланушы порты арқылы қосылсаңыз, онда SQL Server данасының атауымен бірге порт нөмірін үтір арқылы көрсетіңіз, мысалы:

```
SQL_Server_host_name,1433
```

Басқару сервері мен SQL Server сервері арасындағы байланысты сертификат арқылы қорғасаңыз, **SQL сервері үлгісінің атауы** өрісінде сертификат жасау кезінде қолданылған дананың атауын көрсетіңіз. Аталған SQL Server данасын қолдансаңыз, SQL Server данасының атауымен бірге порт нөмірін үтір арқылы көрсетіңіз, мысалы:

```
SQL_Server_name,1433
```

Бір құрылғыда бірнеше SQL Server данасын қолдансаңыз, кері қиғаш сызық арқылы дананың атауын қосымша түрде көрсетіңіз, мысалы:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Корпоративтік желідегі SQL Server үшін Always On функциясы қосулы болса, **SQL сервері үлгісінің атауы** өрісінде қолжетімділік тобының тыңдаушысының атын енгізіңіз. Назар аударыңыз, Always On функциясы қосулы болған кезде Басқару сервері синхронды түрде бекітумен бірге қолжетімділік режимін ғана қолдайды.

- **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

Осы қадамда Kaspersky Security Center орнатып жатқан құрылғыға SQL серверін орнатқыңыз келсе, орнатуды доғарып, SQL серверін орнатқаннан кейін қайта іске қосуыңыз керек. Қолдау көрсетілетін SQL серверлері жүйеге қойылатын талаптарда көрсетілген.

SQL серверін қашықтағы құрылғыға орнатқыңыз келсе, Kaspersky Security Center орнату шеберінің жұмысын тоқтатудың қажеті жоқ. SQL Server серверін орнатыңыз және Kaspersky Security Center орнатуға оралыңыз.

- Алдыңғы қадамда **MySQL немесе MariaDB** таңдалған болсаңыз:
  - **SQL сервері үлгісінің атауы** өрісінде ДҚБЖ үлгінің атауын көрсетіңіз. Әдепкі бойынша, Kaspersky Security Center орнатылатын құрылғының IP мекенжайы қолданылады.
  - **Порт** өрісінде Басқару серверін DBMS серверінің дерекқорына қосу үшін портты көрсетіңіз. Әдепкі бойынша 3306-порт орнатылған.
  - **Дерекқор атауы** өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.
- Алдыңғы қадамда **PostgreSQL немесе Postgres Pro** таңдалған болсаңыз:
  - **PostgreSQL немесе Postgres Pro сервері** өрісінде ДҚБЖ үлгінің атауын көрсетіңіз. Әдепкі бойынша, Kaspersky Security Center орнатылатын құрылғының IP мекенжайы қолданылады.
  - **Порт** өрісінде Басқару серверін ДҚБЖ-не қосу үшін портты көрсетіңіз. Әдепкі бойынша 5432-порт орнатылған.

Дерекқор атауы өрісінде Басқару серверінің ақпаратын орналастыру үшін жасалған дерекқордың атауын белгілеңіз. Әдепкі бойынша, *KAV* мәні көрсетілген.

12-қадам. Түпнұсқалық растама режимін таңдау

Басқару серверін дерекқорларды басқару жүйесіне (ДҚБЖ) қосу кезінде қолданылатын түпнұсқалық растама режимін анықтаңыз.

Таңдалған ДҚБЖ жүйеге байланысты, сіз келесі түпнұсқалық растама режимдерін таңдай аласыз:

- SQL Express немесе Microsoft SQL Server үшін келесі нұсқалардың бірін таңдаңыз:
  - **Microsoft Windows аутентификация режимі**. Бұл жағдайда, құқықтарды тексеру кезінде Басқару серверін іске қосу үшін есептік жазба пайдаланылады.
  - **SQL серверінің аутентификация режимі**. Бұл нұсқа таңдалған жағдайда, құқықтарды тексеру үшін терезеде көрсетілген есептік жазба пайдаланылады. **Есептік жазба** және **Құпиясөз** өрістерін толтырыңыз.

    Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

  Бағдарлама дерекқордың екі түпнұсқалық растама режимі үшін қолжетімді ме екендігін тексереді. Дерекқор қолжетімді болмаса, қате туралы хабар пайда болады және сіз дұрыс есептік деректерді көрсетуіңіз қажет.

  > Басқару серверінің дерекқоры басқа құрылғыда болса және Басқару серверінің есептік жазбасы дерекқордың серверіне қатынаса алмаса, онда Басқару серверін орнату немесе жаңарту кезінде SQL серверінің түпнұсқалық растамасы режимін қолданған жөн. Бұл, дерекқоры бар құрылғы доменде болмаған кезде немесе Басқару сервері LocalSystem есептік жазбасымен орнатылған жағдайда орын алуы мүмкін.

MySQL, MariaDB, PostgreSQL немесе Postgres Pro үшін есептік жазба мен құпиясөзді көрсетіңіз.

13-қадам. Басқару серверін іске қосу үшін есептік жазбаны таңдау

Басқару сервері қызмет ретінде іске қосылатын есептік жазбаны таңдаңыз.

- **Есептік жазбаны автоматты түрде жасау**. Бағдарлама, Басқару серверінің kladminserver қызметі іске қосылатын жергілікті KL-AK-* есептік жазбасын жасайды.

  Ортақ қатынасы бар қалтаны және ДҚБЖ жүйесін Басқару серверімен бір құрылғыға орналастыруды жоспарласаңыз, осы нұсқаны таңдай аласыз.

- **Есептік жазбаны таңдау**. Басқару сервері қызметі (kladminserver) сіз таңдаған есептік жазбамен іске қосылады.

  Мысалы, кез келген шығарылымдағы SQL серверін, соның ішінде басқа құрылғыда орналасқан SQL-express серверін ДҚБЖ ретінде пайдалануды жоспарласаңыз және/немесе ортақ қатынасы бар қалтаны басқа құрылғыда орналастыруды жоспарласаңыз, домендік есептік жазбаны таңдауыңыз қажет болады.

  Kaspersky Security Center бағдарламасы қызметтің басқарылатын есептік жазбаларын (MSA) және қызметтің топтық басқарылатын есептік жазбаларын (gMSA) қолдайды. Доменіңізде осындай есептік жазбалар қолданылса, олардың біреуін Басқару сервері қызметі үшін есептік жазба ретінде таңдай аласыз.

  MSA немесе gMSA таңдамас бұрын, есептік жазбаны Басқару серверін орнатқыңыз келетін құрылғыға орнатуыңыз керек. Есептік жазба әлі орнатылмаған болса, Басқару серверін орнатуды болдырмасаңыз, есептік жазбаны орнатыңыз және Басқару серверін орнатуды қайта іске қосыңыз. Жергілікті құрылғыда қызметтердің басқарылатын есептік жазбаларын орнату туралы қосымша ақпаратты Microsoft ресми құжаттамасынан қараңыз.

  MSA немесе gMSA көрсету үшін:

  1. **Шолу** түймесін басыңыз.
  2. Пайда болған терезеде **Нысан түрі** түймесін басыңыз.

3. **Қызметтерге арналған есептік жазба** түрін таңдап, **OK** түймесін басыңыз.

4. Қажетті есептік жазбаны таңдап, **OK** түймесін басыңыз.

Сіз таңдаған есептік жазба, қандай ДҚБЖ жүйесін қолдануды жоспарлап жатқаныңызға байланысты әртүрлі құқықтарға ие болуы тиіс.

Қауіпсіздік мақсатында, Басқару сервері іске қосылатын есептік жазбаға артықшылық бермеңіз.

Басқару сервері есептік жазбасын кейін өзгерту мүмкін емес. Басқару серверінің басқа есептік жазбасын пайдалану үшін failover кластерін қайта орнатуыңыз қажет.

14-қадам. Kaspersky Security Center қызметтерін іске қосу үшін есептік жазбаны таңдау

Осы құрылғыда Kaspersky Security Center қызметтері іске қосылатын есептік жазбаны таңдаңыз:

- **Есептік жазбаны автоматты түрде жасау**. Kaspersky Security Center бағдарламасы осы құрылғында kladmins тобында KlScSvc жергілікті есептік жазбасын жасайды. Kaspersky Security Center қызметтері жасалған есептік жазбамен іске қосылатын болады.

- **Есептік жазбаны таңдау**. Kaspersky Security Center қызметтері сіз таңдаған есептік жазбамен іске қосылатын болады.

  Сізге домендік есептік жазбаны таңдау, мысалы, басқа құрылғыда орналасқан қалтада есептерді сақтауды жоспарлап жатсаңыз немесе мұны ұйымыңыздың қауіпсіздік саясаты талап етіп жатса қажет болады. Сонымен қатар, сізге Басқару серверін істен шығуға төзімді кластерге орнату кезінде домендік есептік жазбаны таңдау қажет болуы мүмкін.

Қауіпсіздік мақсатында, қызметтер іске қосылатын есептік жазбаны артықшылықты етпеңіз.

Таңдалған есептік жазбаның астында KSN прокси-сервері (ksnproxy), Kaspersky белсендіру прокси-сервері (klactprx) және Kaspersky белсендіру порталы (klwebsrv) қызметтері іске қосылатын болады.

15-қадам. Ортақ қатынасы бар қалтаны анықтау

Келесі мақсаттар үшін пайдаланылатын ортақ қатынасы бар қалтаның орналасатын жерін және атауын анықтаңыз:

- бағдарламаларды қашықтан орнату үшін қажетті файлдарды сақтау (орнату пакеттерін жасау кезінде файлдар Басқару серверіне көшіріледі);

- жаңарту көзінен Басқару серверіне көшірілетін жаңартуларды орналастыру.

Бұл ресурсқа барлық пайдаланушылар үшін оқуға ортақ қатынасу құқығы ашылады.

Сіз келесі екі нұсқаның бірін таңдай аласыз:

- **Ортақ қатынас бар қалтаны жасау**. Жаңа қалта жасау. Төменде көрсетілген өрістегі қалтаға апаратын жолды көрсетіңіз.

- **Бұрыннан бар ортақ қалтаны таңдау**. Қолданыстағы қалталар ішінен ортақ қатынасы бар қалтаны таңдау.

Ортақ қатынасы бар қалта, орнату жүзеге асырылатын құрылғыда жергілікті түрде, сондай-ақ ұйым желісінің құрамына кіретін клиент құрылғыларының кез келгенінде қашықтан орналастырылуы мүмкін. Ортақ қатынасы бар қалтаны **Шолу** түймесінің көмегімен немесе тиісті өрісте UNC жолын енгізу арқылы қолмен (мысалы, \\server\Share) көрсете аласыз.

Әдепкісінше орнату бағдарламасы Kaspersky Security Center құрамдастарын қамтитын қолданба қалтасында жергілікті KLSHARE ішкі қалтасын жасайды.

Қажет болса, ортақ қатынасы бар қалтаны кейінірек анықтауға болады.

16-қадам. Басқару серверіне қосылу параметрлерін конфигурациялау

Басқару серверіне қосылу параметрлерін конфигурациялаңыз:

- **Порт**

  Басқару серверіне қосылу орындалатын порт нөмірі.

  Әдепкі бойынша 14000-порт орнатылған.

- **SSL порты**

  SSL протоколын қолдана отырып, Басқару серверіне қауіпсіз қосылу жүзеге асырылатын SSL порты нөмірі.

  Әдепкі бойынша 13000-порт орнатылған.

- **Шифрлау кілтінің ұзындығы**

  Шифрлау кілтінің ұзындығын таңдаңыз: 1024 бит немесе 2048 бит.

  1024 биттік ұзындығы бар шифрлау кілті процессорға аз жүктеме түсіреді, бірақ ескірген болып саналады және техникалық сипаттамалары жағынан сенімді түрде шифрлауды қамтамасыз ете алмауы мүмкін. Сондай-ақ, қолданыстағы жабдық 1024 биттік кілт ұзындығы бар SSL сертификаттарымен үйлесімді болмауы мүмкін.

  2048 биттік ұзындығы бар шифрлау кілті заманға сай шифрлау стандарттарына сай келеді. Дегенмен, 2048 биттік шифрлау кілтін пайдалану процессорға қосымша жүктеме түсіруі мүмкін.

  Әдепкі бойынша **2048 бит (жоғары қауіпсіздік)** нұсқасы таңдалған.

Басқару серверіне қосылу параметрлерін кейінірек өзгертуге болады:

- Сізге порт пен SSL порт нөмірлерін Басқару сервері сипаттарындағы **Қосылу порттары** бөлімінде өзгертуге болады. Басқару серверіне қосылу порттары туралы қосымша ақпаратты Kaspersky Security Center пайдаланатын порттар бөлімінен қараңыз.

- Басқару сервері сертификатын klsetsrvcert утилитасымен ауыстырған кезде шифрлау кілтінің ұзындығын `-o RsaKeyLen:<кілт ұзындығы>` параметрі арқылы өзгертуге болады.

17-қадам. Басқару сервері мекенжайын белгілеу

Басқару серверінің мекенжайын белгілеңіз. Сіз келесі нұсқаның бірін таңдай аласыз:

- **DNS домені аты**. Бұл тәсіл, желіде DNS сервері болған кезде және клиент құрылғылары оның көмегімен Басқару серверінің мекенжайын ала алатын жағдайда қолданылады.
- **NetBIOS атауы**. Бұл тәсіл, клиент құрылғылары NetBIOS протоколы арқылы Басқару сервері мекенжайын алса немесе желіде WINS сервері болса қолданылады.
- **IP мекенжайы**. Бұл тәсіл, Басқару серверінде болашақта өзгермейтін статикалық IP мекенжайы болса қолданылады.

18-қадам. Ұялы құрылғыларды қосу үшін Сервер мекенжайы

Орнату шеберінің бұл қадамы Ұялы құрылғыларды басқару құрамдасын орнатуды таңдаған кезде қолжетімді.

Ұялы құрылғыларды қосу мекенжайы терезесінде, жергілікті желіден тыс ұялы құрылғыларды қосу үшін Басқару серверінің сыртқы мекенжайын көрсетіңіз. Басқару серверінің IP мекенжайын немесе DNS (Domain Name System) мекенжайын көрсетуге болады.

19-қадам. Файлдарды мұрағаттан шығарып, қатты дискіге орнату

Kaspersky Security Center құрамдастарын орнату параметрлерін конфигурациялап болғаннан кейін, файлдарды қатты дискіге орнатуды іске қосуға болады.

Орнатуды іске қосу үшін қосымша бағдарламалар қажет болса, орнату шебері **Міндетті құрамдастарды орнату** терезесінде Kaspersky Security Center орнатуды бастамас бұрын хабарлайды. Қажетті бағдарламалар **Келесі** түймесін басқаннан кейін автоматты түрде орнатылады.

Соңғы бетте Kaspersky Security Center-мен жұмыс істеу үшін қандай консольді іске қосу керектігін таңдауға болады:

- **MMC негізіндегі Басқару консолін іске қосу**
- **Kaspersky Security Center Web Console консолін іске қосу**

  Бұл параметр, алдыңғы қадамдардың бірінде Kaspersky Security Center Web Console орнатуды таңдаған жағдайда ғана қолжетімді.

Сондай-ақ Kaspersky Security Center-мен жұмысты бастамай-ақ шеберді жабу үшін **Аяқтау** түймесін басуға болады. Kaspersky Security Center-мен жұмысты кейінірек кез келген уақытта бастауға болады.

Басқару консолін немесе Kaspersky Security Center Web Console веб-консолін бірінші рет іске қосу кезінде, бағдарламаны алғашқы рет конфигурациялай аласыз.

Басқару серверін тыныш режимде орнату

Басқару серверін тыныш режимде орнатуға болады, яғни орнату параметрлерін интерактивті түрде енгізбестен.

Жергілікті құрылғыда Басқару серверін тыныш режимде орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімді оқып шықсаңыз және оның шарттарын қабылдасаңыз, төмендегі пәрменді қолданыңыз.

2. Құпиялық саясатын оқып шығыңыз. Менің деректерім Құпиялылық саясатында сипатталғандай өңделетінін және берілетінін (соның ішінде үшінші елдерге) түсініп, онымен келіссеңіз ғана төмендегі пәрменді пайдаланыңыз.

3. Келесі пәрменді орындаңыз:

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
```

мұндағы `setup_parameters` – бір-бірінен бос орынмен бөлінген параметрлер мен олардың мәндерінің тізімі (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Setup.exe файлы Kaspersky Security Center дистрибутивінің ішіндегі Server қалтасында орналасқан.

Басқару серверін тыныш режимде орнату кезінде қолдануға болатын параметрлердің аттары мен ықтимал мәндері төмендегі кестеде келтірілген.

Басқару серверін тыныш режимде орнату параметрлері

Параметрдің атауы	Параметрдің сипаттамасы	Қолжетімді мәндері
EULA	Лицензиялық келісімнің шарттарымен келісу.	• 1 – Мен Лицензиялық келісімді толығымен оқып шыққанымды және оның шарттарын қабылдайтынымды растаймын. • Басқа мән немесе белгіленбеген – Лицензиялық келісімнің шарттарымен келіспейсіз (орнату жүзеге асырылмайды).
PRIVACYPOLICY	Құпиялық саясатының шарттарымен келісу.	• 1 – Менің деректерім Құпиялылық саясатында сипатталғандай өңделетінін және тасымалданатынын (соның ішінде үшінші тараптарға) білемін және оған келісемін. Құпиялылық саясатын толықтай оқып, түсінгенімді растаймын. • Басқа мән немесе белгіленбеген – Мен Құпиялылық саясатының шарттарын қабылдамаймын (орнату орындалмайды).
INSTALLATIONMODETYPE	Басқару серверін орнату түрі.	• Standard – стандартты орнату. • Custom – таңдаулы орнату.
INSTALLDIR	Басқару серверін орнату қалтасына апаратын жол.	Жол мәні.

Параметрдің атауы	Параметрдің сипаттамасы	Қолжетімді мәндері
ADDLOCAL	Орнатуға арналған Басқару сервері құрамдастарының тізімі (үтір арқылы).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Басқару серверін дұрыс орнату үшін жеткілікті құрамдастардың минималды тізімі: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	Желінің өлшемі (желідегі құрылғылар саны).	• NRT_1_100 – 1-ден 100 құрылғыға дейін. • NRT_100_1000 – 101-ден 1000 құрылғыға дейін. • NRT_GREATER_1000 – 1000-нан астам құрылғы.
SRV_ACCOUNT_TYPE	Басқару сервері қызмет ретінде іске қосылатын есептік жазбаны белгілеу тәсілі.	• SrvAccountDefault – есептік жазба автоматты түрде жасалады. • SrvAccountUser – пайдаланушы есептік жазбасы қолмен белгіленген. Бұл жағдайда `SERVERACCOUNTNAME` және `SERVERACCOUNTPWD` параметрлерінің мәндерін белгілеу қажет.
SERVERACCOUNTNAME	Басқару сервері қызмет ретінде іске қосылатын есептік жазбаның атауы. SRV_ACCOUNT_TYPE=SrvAccountUser болса, параметр мәнін белгілеу керек.	Жол мәні.
SERVERACCOUNTPWD	Басқару сервері қызмет ретінде іске қосылатын есептік жазбаның құпиясөзі. SRV_ACCOUNT_TYPE=SrvAccountUser болса, параметр мәнін белгілеу керек.	Жол мәні.
SERVERCER	Басқару серверінің сертификатына арналған кілттің ұзындығы (бит түрінде).	• 1 – Басқару серверінің сертификатына арналған кілттің ұзындығы 2048 битті құрайды. • Мән белгіленбеген – Басқару серверінің сертификатына арналған кілттің ұзындығы 1024 битті құрайды.
DBTYPE	Басқару серверінің ақпараттық дерекқорын орналастыру үшін пайдаланылатын дерекқордың түрі. Бұл параметр міндетті болып саналады.	• MySQL – MySQL немесе MariaDB дерекқоры қолданылады. Бұл жағдайда `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` және `MYSQLACCOUNTPWD` параметрлерінің мәндерін көрсетуіңіз керек. • MSSQL – Microsoft SQL Server (SQL Express) дерекқоры қолданылады. Бұл жағдайда, `MSSQLSERVERNAME`, `MSSQLDBNAME`, `MSSQLAUTHTYPE` параметрлерінің мәндерін белгілеу керек. • POSTGRES – PostgreSQL немесе Postgres Pro дерекқоры пайдаланылады. Бұл жағдайда, `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` және `POSTGRESACCOUNTPWD` параметрлері мәндерін белгілеу керек.
MYSQLSERVERNAME	SQL Server толық атауы. DBTYPE=MySQL болса, параметр мәнін белгілеу керек.	Жол мәні.
MYSQLSERVERPORT	SQL серверіне қосылуға арналған порт нөмірі. DBTYPE=MySQL болса, параметр мәнін белгілеу керек.	Сандық мән.
MYSQLDBNAME	Басқару сервері деректерін орналастыру үшін жасалатын дерекқор атауы. DBTYPE=MySQL болса, параметр мәнін белгілеу керек.	Жол мәні.
MYSQLACCOUNTNAME	Дерекқорға қосылуға арналған есептік жазба атауы. DBTYPE=MySQL болса, параметр мәнін белгілеу керек.	Жол мәні.
MYSQLACCOUNTPWD	Дерекқорға қосылуға арналған есептік жазба құпиясөзі. DBTYPE=MySQL болса, параметр мәнін белгілеу керек.	Жол мәні.
MSSQLSERVERNAME	SQL Server толық атауы. DBTYPE=MSSQL болса, параметр мәнін белгілеу керек.	Жол мәні.

Параметрдің атауы	Параметрдің сипаттамасы	Қолжетімді мәндері
MSSQLDBNAME	Дерекқор атауы. DBTYPE=MSSQL болса, параметр мәнін белгілеу керек.	Жол мәні.
MSSQLAUTHTYPE	SQL серверіне қосылу кезінде авторизация түрі. DBTYPE=MSSQL болса, параметр мәнін белгілеу керек.	• Windows – Microsoft Windows аутентификациясы режимі. • SQLServer – SQL серверінің аутентификация режимі. Бұл жағдайда, `MSSQLACCOUNTNAME` және `MSSQLACCOUNTPWD` параметрлерінің мәндерін белгілеу қажет.
MSSQLACCOUNTNAME	SQL серверіне қосылуға арналған есептік жазба атауы. MSSQLAUTHTYPE=SQLServer болса, параметр мәнін белгілеу керек.	Жол мәні.
MSSQLACCOUNTPWD	SQL серверіне қосылуға арналған есептік жазба құпиясөзі. MSSQLAUTHTYPE=SQLServer болса, параметр мәнін белгілеу керек.	Жол мәні.
CREATE_SHARE_TYPE	Ортақ қатынасы бар қалтаны белгілеу тәсілі.	• Create – ортақ қатынасы бар жаңа қалтаны жасау. Бұл жағдайда, `SHARELOCALPATH` және `SHAREFOLDERNAME` параметрлерінің мәндерін белгілеу қажет. • ChooseExisting – бұрыннан бар қалтаны таңдау. Бұл жағдайда, `EXISTSHAREFOLDERNAME` параметрінің мәнін белгілеу қажет.
SHARELOCALPATH	Жергілікті қалтаға апаратын жол. Параметр мәнін белгілеу керек, егер CREATE_SHARE_TYPE=Create	Жол мәні.
SHAREFOLDERNAME	Ортақ қатынасы бар қалтаның желілік атауы. CREATE_SHARE_TYPE=Create болса, параметр мәнін белгілеу керек.	Жол мәні.
EXISTSHAREFOLDERNAME	Қолданыстағы ортақ қатынасы бар қалтаға апаратын толық жол. CREATE_SHARE_TYPE=ChooseExisting болса, параметр мәнін белгілеу керек.	Жол мәні.
SERVERPORT	Басқару серверіне қосылуға арналған порт нөмірі.	Сандық мән.
SERVERSSLPORT	SSL протоколын пайдаланып Басқару серверіне қауіпсіз қосылуға арналған порт нөмірі	Сандық мән.
SERVERADDRESS	Басқару сервері мекенжайы.	Жол мәні.
MOBILESERVERADDRESS	Ұялы құрылғыларды қосу үшін Сервер мекенжайы.	Жол мәні.

Басқару серверін орнату параметрлері Таңдаулы орнатылым бөлімінде егжей-тегжейлі сипатталған.

Басқару консолін әкімшінің жұмыс орнына орнату

Басқару консолін әкімші жұмыс станциясына бөлек орнатуға және осы консоль арқылы желі бойынша Басқару серверін басқаруға болады.

Басқару консолін әкімшінің жұмыс станциясына орнату үшін:

1. setup.exe орындалатын файлын іске қосыңыз.

   Орнату үшін Kaspersky бағдарламалары таңдалатын терезе ашылады.

2. **Тек Kaspersky Security Center Басқару консолін орнату** сілтемесі бойынша бағдарламаларды таңдау терезесінде Басқару консолін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Мақсатты қалтаны таңдаңыз. Әдепкі бойынша, бұл <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Мұндай қалта болмаса, ол орнату барысында автоматты түрде жасалады. Сіз мақсатты қалтаны **Шолу** түймесі арқылы өзгерте аласыз.

4. Орнату шеберінің соңғы терезесінде, Басқару консолін орнату процесін бастау үшін **Іске қосу** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін, Басқару консолі әкімшінің жұмыс станциясына орнатылады.

Басқару консолін әкімші жұмыс станциясына тыныш режимде орнату үшін:

1. Лицензиялық келісімді оқып шығыңыз. Лицензиялық келісімді оқып шықсаңыз және оның шарттарын қабылдасаңыз, төмендегі пәрменді қолданыңыз.

2. Kaspersky Security Center дистрибутивінің `Distrib\Console` қалтасында келесі пәрменнің көмегімен setup.exe файлын іске қосыңыз:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Басқару консолімен бірге `Distrib\Console\Plugins` қалтасындағы барлық басқару плагиндерін орнатқыңыз келсе, келесі пәрменді орындаңыз:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Басқару консолімен бірге `Distrib\Console\Plugins` қалтасынан қандай басқару плагиндерін орнату керектігін білгіңіз келсе, "/p" кілтінен кейін басқару плагиндерін көрсетіп, оларды үтірлі нүктемен бөліңіз:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   Мұндағы `P1`, `P2`, `P3` – `Distrib\Console\Plugins` қалтасындағы басқару плагиндері қалталарының атауына сай келетін басқару плагиндері атауы. Мысалы:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

Басқару консолі және басқару плагиндері (егер олар көрсетілген болса) әкімшінің жұмыс станциясына орнатылады.

Басқару консолі орнатылғаннан кейін, Басқару серверіне қосылу керек. Ол үшін Басқару консолін іске қосып, ашылған терезеде Басқару сервері орнатылған құрылғының атауын немесе құрылғының IP мекенжайын, сондай-ақ оған қосылу үшін есептік жазба параметрлерін көрсету керек. Басқару серверімен байланыс орнатылғаннан кейін, осы Басқару консолі арқылы антивирустық қорғаныс жүйесін басқаруға болады.

Басқару консолін Microsoft Windows бағдарламаларын орнату және жоюдың стандартты құралдарымен жоюға болады.

Kaspersky Security Center орнатқаннан кейін жүйеде орын алған өзгерістер

Басқару консолінің белгішесі

Басқару консолін орнату нәтижесінде сіздің құрылғыда Басқару консолін іске қосу белгішесі пайда болады. **Бастау** → **Бағдарламалар** → **Kaspersky Security Center** мәзірінде Басқару консолін таба аласыз.

Басқару сервері және Желілік агент қызметтері

Басқару сервері мен Желілік агент құрылғыға төмендегі кестеде көрсетілген сипаттары бар қызметтер ретінде орнатылады. Кестеде Басқару сервері орнатылғаннан кейін құрылғыда орындалатын басқа қызметтердің атрибуттары да көрсетілген.

Kaspersky Security Center қызметтерінің сипаттары

Құрамдас	Қызмет атауы	Қызметтің көрсетілетін атауы	Есептік жазба
Басқару сервері	kladminserver	Kaspersky Security Center Басқару сервері	Пайдаланушы көрсеткен немесе арнайы, орнату кезінде жасалған, артықшылықсыз KL-AK-* түріндегі есептік жазба
Желілік агент	klnagent	Kaspersky Security Center Желілік агенті	Жергілікті жүйе
Kaspersky Security Center Web Console жұмыс істеуіне және ұйымның ішкі порталын ұйымдастыруға арналған веб-сервер	klwebsrv	Kaspersky веб-сервері	Арнайы артықшылықсыз KlScSvc есептік жазбасы
Белсендіру прокси-сервері	klactprx	Kaspersky белсендіру прокси-сервері	Арнайы артықшылықсыз KlScSvc есептік жазбасы
KSN прокси-сервері	ksnproxy	Kaspersky Security Network прокси-сервері	Арнайы артықшылықсыз KlScSvc есептік жазбасы

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйіндеріне орнатсаңыз, klfocsvc_klfoc қызметі қолжетімді болады. klnagent_klfoc және klfocsvc_klfoc қызметтері жергілікті жүйе тіркелгісі арқылы іске қосылады. kladminserver_klfoc қызметі "ksc" тіркелгісі бойынша іске қосылуы керек; басқа қызметтер – "rightless" тіркелгісі арқылы. "ksc" және "rightless" тіркелгілері жергілікті әкімші құқықтары бар KLAdmins тобына қосылуы керек. Kaspersky Security Center дұрыс жұмыс істеуі үшін, қызметтерді іске қосу үшін тек "ksc" және "rightless" тіркелгілерін пайдалану керек. Сондай құқықтары бар басқа тіркелгілерді пайдалану ұсынылмайды. Төмендегі кестеде ақауларға төзімді Kaspersky Security Center кластерінде басқару серверін орнатқаннан кейін құрылғыда қолданылатын қызметтердің сипаттары көрсетілген.

Ақауларға төзімді Kaspersky Security Center кластерінде орнатылған Kaspersky Security Center қызметтерінің сипаттары

Құрамдас	Қызмет атауы	Қызметтің көрсетілетін атауы	Есептік жазба
Басқару сервері	kladminserver_klfoc	Kaspersky Security Center Басқару сервері	ksc
Желілік агент	klnagent_klfoc	Kaspersky Security Center Желілік агенті	Жергілікті жүйе
Kaspersky Security Center Web Console жұмыс істеуіне және ұйымның ішкі порталын ұйымдастыруға арналған веб-сервер	klwebsrv_klfoc	Kaspersky веб-сервері	rightless
Белсендіру прокси-сервері	klactprx_klfoc	Kaspersky белсендіру прокси-сервері	rightless
KSN прокси-сервері	ksnproxy_klfoc	Kaspersky Security Network прокси-сервері	rightless
Ақауларға төзімді Kaspersky Security Center кластері	klfocsvc_klfoc	Ақауларға төзімді Kaspersky Security Center кластері	Жергілікті жүйе

Kaspersky Security Center Web Console қызметтері

Егер сіз құрылғыға Kaspersky Security Center Web Console орнатсаңыз, онда келесі қызметтер орындалады (төмендегі кестені қараңыз):

Kaspersky Security Center Web Console қызметтері

Қызметтің көрсетілетін атауы	Есептік жазба
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Желілік қызмет
Kaspersky Security Center Product Plugins Server	NT Service/KSCWebConsolePlugin
Kaspersky Security Center Web Console Management Service	Жергілікті жүйе
Kaspersky Security Center Web Console Message Queue	NT Service/KSCWebConsoleMessageQueue

Желілік агенттің серверлік нұсқасы

Басқару серверімен бірге құрылғыға Желілік агенттің серверлік нұсқасы орнатылады. Ол Басқару серверінің құрамына кіреді, оның құрамында орнатылады және жойылады және тек жергілікті түрде орнатылған Басқару серверімен ғана әрекеттесе алады. Агенттің Басқару серверіне қосылу параметрлерін конфигурациялау қажет емес: құрамдастар бір құрылғыда орнатылғанын ескере отырып, орнату бағдарламалық түрде іске асырылған. Желілік агенттің серверлік нұсқасы бірдей атрибуттармен орнатылады және стандартты Желілік агент сияқты бағдарламаларды басқару функцияларын орындайды. Бұл нұсқада Басқару серверінің клиент құрылғысы қосылған басқару тобының саясаты әрекет етеді. Желілік агенттің серверлік нұсқасы үшін Серверді ауыстыру тапсырмасын қоспағанда, Желілік агент үшін қарастырылған барлық тапсырмалар жасалады.

Желілік агентті Басқару сервері бар құрылғыға бөлек орнату мүмкін емес.

Сіз Сервер мен Желілік агент қызметтерінің сипаттарын көре аласыз, сонымен қатар олардың жұмысын Microsoft Windows стандартты басқару құралдарының көмегімен қадағалай аласыз: Компьютерді басқару\Қызметтер. Басқару сервері қызметінің жұмысы туралы ақпарат Microsoft Windows жүйелік журналында, Басқару сервері орнатылған құрылғыда, Kaspersky Event журналының жеке тармағында сақталады.

Қызметтерді қолмен іске қосу және өшіру және қызмет конфигурацияларында есептік жазбаларды ауыстыру ұсынылмайды. Қажет болса, klsrvswch утилитасының көмегімен Басқару сервері қызметінің есептік жазбасын ауыстыруға болады. klsrvswch утилитасын Басқару серверін орнату үшін пайдаланылған әкімші құқықтары бар есептік жазба арқылы Басқару сервері құрылғысында іске қосу керек екенін ескеріңіз.

Есептік жазбалар және қауіпсіздік топтары

Әдепкі бойынша Басқару сервері инсталляторы келесі есептік жазбаларды жасайды:

- KL-AK-*: Басқару сервері қызметінің есептік жазбасы;
- KlScSvc: Басқару сервері құрамындағы басқа қызметтерге арналған есептік жазба;
- KlPxeUser: операциялық жүйелерді орналастыруға арналған есептік жазба.

Егер орнату кезеңінде сіз Басқару сервері қызметі және басқа қызметтер үшін басқа есептік жазбаларды таңдасаңыз, онда сіз көрсеткен есептік жазбалар пайдаланылады.

Басқару сервері орнатылған құрылғыда тиісті құқықтар жиынтығы бар KLAdmins және KLOperators жергілікті қауіпсіздік топтары автоматты түрде жасалады.

Басқару серверін домен контроллеріне орнату ұсынылмайды; дегенмен домен контроллеріне басқару серверін орнатсаңыз, орнатушыны домен әкімшісі құқықтарымен бастау керек. Бұл жағдайда, орнату бағдарламасы автоматты түрде KLAdmins және KLOperators домендік қауіпсіздік топтарын жасайды. Домен контроллері емес құрылғыға басқару серверін орнатсаңыз, жергілікті әкімші құқықтарымен орнату бағдарламасын іске қосуыңыз керек. Бұл жағдайда, орнату бағдарламасы автоматты түрде KLAdmins және KLOperators жергілікті қауіпсіздік топтарын жасайды.

Электрондық пошта арқылы хабарландыруларды конфигурациялаған кезде ESMTP аутентификациясы үшін пошта серверінде есептік жазба қажет болып қалуы мүмкін.

Бағдарламаны жою

Сіз Kaspersky Security Center бағдарламасын Microsoft Windows бағдарламаларын орнату және жоюдың стандартты құралдарымен жоя аласыз. Бағдарламаны жою үшін шебер іске қосылады, оның жұмысы нәтижесінде құрылғыдан бағдарламаның барлық құрамдастары (плагиндерді қоса) жойылады. Шебер сіздің әдепкі бойынша браузеріңізде веб-бетті сауалнамамен бірге ашып, онда сіз Kaspersky Security Center-ді пайдалануды неге тоқтатуға шешім қабылдағаныңызды айта аласыз. Егер шебер жұмыс істеп тұрған кезде ортақ қатынасы бар қалтаны (KLSHARE) жоюды белгілемеген болсаңыз, оған қатысты барлық тапсырмаларды аяқтағаннан кейін, оны қолмен жоюға болады.

Бағдарлама жойылғаннан кейін, файлдар жүйелік уақытша қалтада қалуы мүмкін.

Бағдарламаларды жою тапсырмаларын жасау шебері Басқару серверінің сақтық көшірмесін сақтауды ұсынады.

Бағдарламаны Microsoft Windows 7 және Microsoft Windows 2008 операциялық жүйелерінен жойған кезде бағдарламаларды жою тапсырмаларын жасау шеберінің жұмысы мерзімінен бұрын аяқталуы мүмкін. Бұған жол бермеу үшін, операциялық жүйеде есептік жазбаларды басқару қызметін (UAC) өшіріп, бағдарламаны жоюды қайта іске қосыңыз.

Kaspersky Security Center алдыңғы нұсқасын жаңарту туралы

Бұл бөлімде Kaspersky Security Center бағдарламасын алдыңғы нұсқадан қалай жаңартуға болатындығы туралы ақпарат бар. Kaspersky Security Center бағдарламасы жергілікті түрде немесе Kaspersky Security Center ақауларға төзімді кластерінің түйіндерінде орнатылғанына байланысты, Kaspersky Security Center-ді әртүрлі тәсілдермен жаңарта аласыз.

Жаңарту кезінде ДҚБЖ жүйесін Басқару сервері және басқа бағдарламамен ортақ пайдалануға жол берілмейді.

Басқару серверін 15.1 нұсқасына жаңартсаңыз, Желілік агент 15 немесе одан төмен нұсқасы үшін орнату пакеттерін жасай алмайтыныңызды ескеріңіз. Бұрын жасалған орнату пакеттері қолжетімді болады.

Kaspersky Security Center бағдарламасының алдыңғы нұсқасын жаңарту кезінде Kaspersky қолдау көрсетілетін бағдарламаларының барлық орнатылған плагиндері сақталады. Басқару сервері плагині және Желілік агент плагині автоматты түрде жаңартылады (Басқару консолі үшін де, Kaspersky Security Center Web Console үшін де).

Kaspersky Security Center алдыңғы нұсқасын жаңарту

Келесі бөлімде жаңартуға дайындалу үшін ұсынылған қадамдар сипатталады: Kaspersky Security Center және басқарылатын қауіпсіздік бағдарламаларын жаңарту.

Басқару серверінің алдыңғы нұсқасы орнатылған құрылғыға басқару серверінің 15.1 нұсқасын орнатуға болады (11 (11.0.0.1131b) нұсқасынан бастап). 15.1 нұсқасына дейін жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Басқару серверін орнату кезінде қиындықтар туындаса, жаңарту алдында жасалған Сервер деректерінің сақтық көшірмесін пайдаланып Басқару серверінің алдыңғы нұсқасын қалпына келтіруге болады.

Егер желіде Басқару серверінің кем дегенде бір жаңа нұсқасы орнатылған болса, сіз желідегі басқа Басқару серверлерін Басқару серверінің орнату пакетін пайдаланатын қашықтан орнату тапсырмасы арқылы жаңарта аласыз.

Ақауларға төзімді Kaspersky Security Center кластерін орналастырған болсаңыз, оның түйіндерінде Kaspersky Security Center жаңартуға да болады.

Басқару серверін алдыңғы нұсқадан 15.1-нұсқаға дейін жаңарту үшін:

1. 15.1 нұсқасы үшін ksc_15.1_<жинақ нөмірі>_full_<локализация тілі>.exe орындалатын файлын іске қосыңыз (бұл файлды Kaspersky сайтынан жүктеп ала аласыз).

2. Ашылған терезеде **Kaspersky Security Center бағдарламасын орнату** сілтемесі арқылы Басқару серверін орнату шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Лицензиялық келісім мен Құпиялық саясатымен танысыңыз. Лицензиялық келісім мен Құпиялық саясатының барлық тармақтарымен келіссеңіз, **Толығымен оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** блогында келесі жалаушаларды қойыңыз:

   - **Осы Лицензиялық келісімнің ережелері мен шарттары**
   - **Деректердің өңделуін сипаттайтын Құпиялылық саясаты**

   Бағдарламаны орнату келесі екі жалаушаны қойғаннан кейін жалғасады. Орнату шебері сізге ерте нұсқалар үшін Басқару сервері деректерінің сақтық көшірмесін жасауды ұсынады.

   Kaspersky Security Center бағдарламасы Басқару серверінің бұрынғы нұсқасы жасаған сақтық көшірмеден деректерді қалпына келтіруді қолдайды.

4. Басқару сервері деректерінің сақтық көшірмесін жасағыңыз келсе, мұны ашылған **Басқару сервері деректерінің резервтік қоймасы** терезесінде көрсетіңіз.

   Деректердің сақтық көшірмесін klbackup утилитасы жасайды. Бұл утилита бағдарламаның дистрибутиві құрамына кіреді және Kaspersky Security Center орнату қалтасы түбірінде орналасады.

5. Орнату шеберінің нұсқауларын орындау арқылы Басқару серверінің 15.1 нұсқасын орнатыңыз.

   Егер Kaspersky Security Center Web Console қызметі бос емес екендігі туралы хабар пайда болса, шебер терезесінде **Елемеу** түймесін басыңыз.

   > Орнату шеберінің жұмысын тоқтату ұсынылмайды. Басқару серверін орнату сатысында жаңарту процесін тоқтату Kaspersky Security Center жаңа нұсқасының жұмыс істемеуіне әкелуі мүмкін.

6. Алдыңғы нұсқаның Желілік агенті орнатылған құрылғылар үшін Желілік агенттің жаңа нұсқасын қашықтан орнату тапсырмасын жасаңыз және іске қосыңыз.

   > Linux үшін Желілік агентті Kaspersky Security Center нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

   Қашықтан орнату тапсырмасын орындағаннан кейін Желілік агент нұсқасы жаңартылды.

   Енді қажет емес тәуелділіктерді жою үшін Linux негізіндегі активтерде келесі пәрмендерді орындаңыз:

   - Debian негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - RPM негізіндегі активтер үшін келесі пәрмендердің бірін іске қосыңыз:
     - `dnf autoremove`
     - `yum autoremove`

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйінінде жаңарту

Басқару серверінің 15.1 нұсқасын басқару серверінің анағұрлым ерте нұсқасы орнатылған (13.2 нұсқасынан бастап) ақауларға төзімді Kaspersky Security Center кластерінің әрбір түйініне орната аласыз. 15.1 нұсқасына дейін жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Егер сіз бұрын Kaspersky Security Center бағдарламасын жергілікті құрылғыларға орнатқан болсаңыз, онда сіз осы құрылғыларда Kaspersky Security Center жаңарта аласыз.

Kaspersky Security Center бағдарламасын ақауларға төзімді Kaspersky Security Center кластерінің түйінінде жаңарту үшін:

1. Белсенді кластер түйінінде келесі әрекеттерді орындаңыз:

   a. ksc_15.1.<жинақ нөмірі>_full_<локализация тілі>.exe орындалатын файлын іске қосыңыз.

      Жаңарту үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. Басқару серверін орнату шеберін іске қосу үшін **Kaspersky Security Center Басқару серверін орнату** сілтемесінен өтіңіз. Шебердің нұсқауларын орындаңыз.

   b. Лицензиялық келісім мен Құпиялық саясатымен танысыңыз. Лицензиялық келісім мен Құпиялық саясатының барлық тармақтарымен келіссеңіз, **Толығымен оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** блогында келесі жалаушаларды қойыңыз:

      - **Осы Лицензиялық келісімнің ережелері мен шарттары**
      - **Деректердің өңделуін сипаттайтын Құпиялылық саясаты**

      Орнатуды жалғастыру үшін екі жалаушаны қойыңыз.

      Егер сіз Лицензиялық келісімді немесе Құпиялық саясатын қабылдамасаңыз, жаңартуды болдырмау үшін **Бас тарту** түймесін басыңыз.

2. Ақауларға төзімді Kaspersky Security Center кластерінің пассивті түйінінде белсенді түйінмен бірдей әрекеттерді орындаңыз.

3. Кластерді іске қосу.

Нәтижесінде сіз ақауларға төзімді Kaspersky Security Center кластерінің түйіндеріне басқару серверінің соңғы нұсқасын орнаттыңыз.

Ақауларға төзімді Microsoft кластер түйіндеріндегі Kaspersky Security Center орталығын жаңарту

Басқару серверінің нұсқасын басқару серверінің ең ерте (13.2 нұсқасынан бастап) нұсқасы орнатылған ақауларға төзімді Microsoft кластерінің әрбір түйінінде 15.1 нұсқасына дейін жаңартуға болады. 15.1 нұсқасына дейін жаңарту кезінде Басқару серверінің алдыңғы нұсқасының барлық деректері мен параметрлері сақталады.

Ақауларға төзімді Microsoft кластер түйіндерінде Kaspersky Security Center-ді жаңарту үшін кластердің кез келген түйінінде келесі әрекеттерді орындаңыз:

1. ksc_15.1.<жинақ нөмірі>_full_<локализация тілі>.exe орындалатын файлын іске қосыңыз.

   Жаңарту үшін Kaspersky бағдарламалары таңдалатын терезе ашылады. Басқару серверін орнату шеберін іске қосу үшін **Kaspersky Security Center Басқару серверін орнату** сілтемесінен өтіңіз. Шебердің нұсқауларын орындаңыз.

2. Лицензиялық келісім мен Құпиялық саясатымен танысыңыз. Лицензиялық келісім мен Құпиялық саясатының барлық тармақтарымен келіссеңіз, **Толығымен оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** блогында келесі жалаушаларды қойыңыз:

   - **Осы Лицензиялық келісімнің ережелері мен шарттары**
   - **Деректердің өңделуін сипаттайтын Құпиялылық саясаты**

   Орнатуды жалғастыру үшін екі жалаушаны қойыңыз.

   Егер сіз Лицензиялық келісімді немесе Құпиялық саясатын қабылдамасаңыз, жаңартуды болдырмау үшін **Бас тарту** түймесін басыңыз.

3. **Кластерге орнату түрі** терезесінде **Кластер (барлық кластер түйіндерінде орнату)** параметрін таңдаңыз.

   Содан кейін орнатушы барлық кластер түйіндерінде басқару серверінің жаңартуын реттейді және аяқтайды. Жаңарту кезінде басқару серверінің параметрлерін өзгерту мүмкін емес.

Нәтижесінде ақауларға төзімді төзімді Microsoft кластерінің түйіндеріне басқару серверінің соңғы нұсқасын орнаттыңыз.

Kaspersky Security Center бастапқы конфигурациялау

Бұл бөлімде бастапқы конфигурациялау үшін Kaspersky Security Center орнатқаннан кейін орындалатын қадамдар сипатталған.

Қорғанысты күшейту нұсқаулығы

Қорғанысты күшейту нұсқаулығы Kaspersky Security Center бағдарламасын орнататын және басқаратын мамандарға және Kaspersky Security Center пайдаланатын ұйымдарға техникалық қолдау көрсететін мамандарға арналған.

Қорғанысты күшейту нұсқаулығы, бұзылу қаупін азайту үшін Kaspersky Security Center және оның құрамдастарын конфигурациялаудың ұсыныстары мен ерекшеліктерін сипаттайды.

Конфигурациялау алдында басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасын немесе klbackup утилитасын пайдаланып, Kaspersky Security Center басқару серверінің сақтық көшірмесін жасаңыз және оны қауіпсіз жерде сақтаңыз.

Қорғанысты күшейту нұсқаулығы келесі ақпаратты қамтиды:

- Басқару серверін орналастыру схемасын таңдау
- Басқару серверіне қауіпсіз қосылымды конфигурациялау

- Басқару серверімен жұмыс істеу үшін есептік жазбаларды конфигурациялау
- Басқару сервері мен клиент құрылғыларын қорғауды басқару
- Басқарылатын қолданбалар қорғанысын конфигурациялау
- Басқару серверіне техникалық қызмет көрсету
- Үшінші тарап жүйелеріне ақпарат беру

Басқару серверімен жұмыс істеуді бастамас бұрын, Kaspersky Security Center бағдарламасы сізге Қорғанысты күшейту нұсқаулығының қысқаша нұсқасын оқуды ұсынады.

Қорғаныс күшейту нұсқаулығын оқып шыққаныңызды растамайынша, Басқару серверін пайдалана алмайтыныңызды ескеріңіз.

Қорғанысты күшейту нұсқаулығын оқып шығу үшін:

1. Басқару консолін немесе Kaspersky Security Center Web Console веб-консолін ашыңыз және консольге кіріңіз. Консоль Қорғанысты күшейту нұсқаулығының ағымдағы нұсқасын оқып шыққаныңызды растағаныңызды тексереді.

   Қорғанысты күшейту нұсқаулығын әлі оқылмаған болсаңыз, оның қысқаша нұсқасы бар терезе ашылады.

2. Келесі әрекеттердің бірін орындаңыз:

   - Қорғанысты күшейту нұсқаулығының қысқа нұсқасын мәтіндік құжат ретінде көргіңіз келсе, **Жаңа терезеде ашу** сілтемесінен өтіңіз.
   - Қорғанысты күшейту нұсқаулығының толық нұсқасын көргіңіз келсе, **Онлайн анықтамадан Нығайту нұсқаулығын ашу** сілтемесінен өтіңіз.

3. Қорғанысты күшейту нұсқаулығын оқығаннан кейін, **Нығайту нұсқаулығын толық оқып, түсінгенімді растаймын** жалаушасын қойыңыз және **Қабылдау** түймесін басыңыз.

Енді сіз Басқару серверімен жұмыс істей аласыз.

Қорғанысты күшейту нұсқаулығының жаңа нұсқасы пайда болғанда, Kaspersky Security Center оны оқуды ұсынады.

Басқару серверін жылдам іске қосу шебері

Бұл бөлімде Басқару серверін жылдам іске қосу шеберінің жұмысы туралы ақпарат берілген.

Бағдарламаны жылдам іске қосу шебері туралы

Бұл бөлімде Басқару серверін жылдам іске қосу шеберінің жұмысы туралы ақпарат берілген.

Басқару серверін жылдам іске қосу шебері қажетті тапсырмалар мен саясаттардың минималды жиынтығын жасауға, минималды параметрлерді конфигурациялауға, Kaspersky басқарылатын бағдарламалары үшін плагиндерді жүктеуге және орнатуға, және Kaspersky басқарылатын бағдарламалары үшін орнату пакеттерін жасауға мүмкіндік береді. Шебердің жұмысы барысында, сіз бағдарламаға келесі өзгерістерді енгізе аласыз:

- Басқарылатын бағдарламаларға арналған плагиндерді жүктеп алу және орнату. Бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғаннан кейін, орнатылған басқару плагиндерінің тізімі Басқару сервері сипаттары терезесінде **Қосымша** → **Орнатылған бағдарламаны басқару плагиндерінің мәліметтері** бөлімінде көрсетіледі.

- Kaspersky басқарылатын бағдарламалары үшін орнату пакеттерін жасаңыз. Бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғаннан кейін, Windows операциялық жүйесі мен Kaspersky басқарылатын бағдарламалары үшін Желілік агенттің орнату пакеттері **Басқару сервері** → **Қосымша** → **Қашықтан орнату** → **Орнату пакеттері** тізімінде көрсетіледі.

- Басқару топтарындағы құрылғыларға автоматты түрде таратуға болатын кілт файлдарын қосу немесе белсендіру кодтарын енгізу. Бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғаннан кейін, лицензиялық кілттер туралы ақпарат **Басқару сервері** → **Kaspersky лицензиялары** тізімінде және Басқару сервері сипаттары терезесінің **Лицензиялық кілттер** бөлімінде көрсетіледі.

- Kaspersky Security Network (KSN) желісімен өзара әрекетті конфигурациялау.

- Басқару сервері мен басқарылатын бағдарламалардың жұмысындағы оқиғалар туралы хабарландыруларды электрондық пошта арқылы таратуды конфигурациялаңыз (хабарландыру сәтті түрде келуі үшін Басқару серверінде және барлық алушы құрылғыларда Messenger хабар қызметі іске қосылуы керек). Бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғаннан кейін, пошталық хабарландырулар параметрлері **Хабарландыру** бөлімінде, Басқару сервері сипаттары терезесінде көрсетіледі.

- Құрылғыларда орнатылған бағдарламалардың осалдықтарын түзету және жаңарту параметрлерін конфигурациялау.

- Жұмыс станциялары мен серверлерді қорғау саясатын, сондай-ақ зиянды БҚ іздеу, жаңартуларды алу және басқарылатын құрылғылар иерархиясының жоғарғы деңгейі үшін деректерді сақтық көшірмелеу тапсырмаларын қалыптастыру. Бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғаннан кейін, жасалған тапсырмалар **Басқару сервері** → **Тапсырмалар** тізімінде көрсетіледі, ал басқарылатын бағдарламалардың плагиндеріне сай келетін саясаттар **Басқару сервері** → **Саясаттар тізімінде** көрсетіледі.

Бағдарламаны жылдам іске қосу шебері, егер мұндай саясаттар бұрын **Басқарылатын құрылғылар** тобы үшін жасалмаған болса, Kaspersky Endpoint Security for Windows сияқты басқарылатын бағдарламалар үшін саясаттарды жасайды. **Басқарылатын құрылғылар** тобында бірдей аттары бар тапсырмалар болмаса, Бағдарламаны жылдам іске қосу шебері тапсырмалар жасайды.

Басқару консолінде Kaspersky Security Center бағдарламасы бағдарламаны бірінші рет іске қосқаннан кейін, бағдарламаны жылдам іске қосу шеберін іске қосуды ұсынады. Сондай-ақ, бағдарламаны жылдам іске қосу шеберін кез келген уақытта қолмен іске қоса аласыз.

Басқару серверін жылдам іске қосу шеберін іске қосу

Серверге бірінші рет қосылу кезінде Басқару серверін орнатқаннан кейін, бағдарлама автоматты түрде бағдарламаны жылдам іске қосу шеберін іске қосуды ұсынады. Сондай-ақ, бағдарламаны жылдам іске қосу шеберін кез келген уақытта қолмен іске қоса аласыз.

Бағдарламаны жылдам іске қосу шеберін қолмен іске қосу үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Түйіннің мәнмәтіндік мәзірінде **Барлық тапсырмалар → Басқару серверін жылдам іске қосу шебері** тармағын таңдаңыз.

Шебер Басқару серверін бастапқы конфигурациялауды ұсынады. Содан кейін, шебердің нұсқауларын орындаңыз.

Бағдарламаны жылдам іске қосу шеберін қайтадан іске қосқан кезде, шеберді өткен жолы іске қосқан кезде жасалған тапсырмалар мен саясаттар қайта жасалмайды.

1-қадам. Прокси-сервер параметрлерін конфигурациялау

Басқару серверінің интернетке қатынасу параметрлерін көрсетіңіз. Kaspersky Security Network пайдалану, сондай-ақ Kaspersky Security Center және Kaspersky басқарылатын бағдарламалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.

Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін таңдаңыз. Параметр таңдалған болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

- **Мекенжай**

  Kaspersky Security Center-ді интернетке қосу үшін прокси-сервер мекенжайы.

- **Порт нөмірі**

  Kaspersky Security Center прокси-қосылымы орнатылатын порт нөмірі.

- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Жергілікті желідегі құрылғыларға қосылған кезде прокси-сервер қолданылмайды.

- **Прокси-сервердегі түпнұсқалық растама**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

- **Пайдаланушы аты**

  Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Интернетке қатынасуды, бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, кейінірек конфигурациялай аласыз.

2-қадам. Бағдарламаны белсендіру тәсілін таңдау

Kaspersky Security Center белсендірудің келесі нұсқаларының бірін таңдаңыз:

- **Белсендіру кодын енгізіңіз**

  Белсендіру коды – жиырма латын әрпі мен санынан құралған бірегей бірізділік. Сіз Kaspersky Security Center бағдарламасын белсендіретін кілтті қосу үшін белсендіру кодын енгізесіз. Белсендіру коды сізге Kaspersky Security Center сатып алу кезінде көрсетілген электрондық пошта мекенжайына жіберіледі.

  Бағдарламаны белсендіру кодының көмегімен белсендіру үшін, Kaspersky белсендіру серверлеріне қосылу мақсатында интернетке қатынасу талап етіледі.

  Бағдарламаны белсендіру үшін осы нұсқаны таңдасаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосуға болады.

  Осы нұсқа таңдалса, лицензиялық кілт басқарылатын құрылғыларға таратылатын болады.

  Осы нұсқа таңдалмаса, лицензиялық кілтті басқарылатын құрылғыларға, басқару консолі шежіресінің **Kaspersky лицензиялары** қалтасында кейінірек таратуға болады.

  > Егер қандай да бір себептермен белсендіру кодын пайдаланып белсендіру сәтсіз аяқталса, кілт файлын көрсету арқылы бағдарламаны белсендіруге болады.

- **Кілт файлын көрсетіңіз**

  Кілт файлы – Kaspersky сізге ұсынатын key кеңейтімі бар файл. Кілт файлы бағдарламаны белсендіретін кілтті қосуға арналған.

  Кілт файлын алу әдістері Кілт файлы туралы ақпарат бөлімде сипатталған.

  Бағдарламаны кілт файлы арқылы белсендіру үшін Kaspersky белсендіру серверлеріне қосылудың қажет емес.

  Бағдарламаны белсендіру үшін осы нұсқаны таңдасаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосуға болады.

  Осы нұсқа таңдалса, лицензиялық кілт басқарылатын құрылғыларға таратылатын болады.

  Осы нұсқа таңдалмаса, лицензиялық кілтті басқарылатын құрылғыларға, басқару консолі шежіресінің **Kaspersky лицензиялары** қалтасында кейінірек таратуға болады.

- **Бағдарламаны белсендіруді кейінге қалдырыңыз**

  Бағдарлама Базалық функционалдылық режимінде, Ұялы құрылғыларды басқару және Осалдықтар мен патчтарды басқару қызметінің қолдауынсыз жұмыс істейтін болады.

Бағдарламаны белсендіруді кейінге қалдыруды таңдаған болсаңыз, кейінірек кез келген уақытта лицензиялық кілтті қоса аласыз.

3-қадам. Қорғаныс аумағы мен операциялық жүйелерді таңдау

Желіңізде қолданылатын қорғаныс аумақтары мен операциялық жүйелерді таңдаңыз. Осы параметрлерді таңдағанда, желіңіздегі клиент құрылғыларына орнату үшін жүктеуге болатын Kaspersky серверлеріндегі бағдарламаларды басқару плагиндері мен дистрибутивтеріне арналған сүзгілерді көрсетесіз. Келесі параметрлерді таңдаңыз:

- **Аймақтар**

  Сіз келесі қорғаныс аймақтарының бірін таңдай аласыз:

  - **Жұмыс станциялары**. Желідегі жұмыс станцияларын қорғағыңыз келсе, осы параметрді таңдаңыз. Әдепкі бойынша Жұмыс станциясы параметрі таңдалған.

  - **Файлдық серверлер және сақтау орны**. Желіңіздегі файл серверлерін қорғағыңыз келсе, осы параметрді таңдаңыз.

  - **Ұялы құрылғылар**. Ұйымыңызға немесе ұйымыңыздағы қызметкерлерге тиесілі мобильдік құрылғыларды қорғағыңыз келсе, осы параметрді таңдаңыз. Бұл параметрді таңдаған болсаңыз, бірақ Мобильдік құрылғыларды басқару мүмкіндігі бар лицензияны бермеген болсаңыз, мобильдік құрылғыларды басқару мүмкіндігі бар лицензияны беруді сұрайтын хабар көрсетіледі. Бұл лицензиясыз мобильдік құрылғыны басқару мүмкіндіктерін пайдалана алмайсыз.

  - **Виртуалдандыру**. Желіңіздегі виртуалды машиналарды қорғағыңыз келсе, осы параметрді таңдаңыз.

  - **Анти-спам**. Ұйымыңыздағы пошта серверлерін спамнан, алаяқтықтан және зиянды бағдарламаларды жеткізуден қорғағыңыз келсе, осы опцияны таңдаңыз.

- **Операциялық жүйелер**

  Сіз келесі платформалардың бірін таңдай аласыз:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Басқа

  Қолдау көрсетілетін операциялық жүйелер үшін Аппараттық және бағдарламалық талаптар бөлімін қараңыз.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қолжетімді орнату пакеттерінің тізімінен Kaspersky бағдарламаларының орнату пакеттерін таңдауға болады. Қажетті орнату пакеттерін табуды жеңілдету үшін қолжетімді орнату пакеттерінің тізімін келесі критерийлер бойынша сүзуге болады:

- қауіпсіз аймақ;
- жүктелетін бағдарламалық жасақтама түрі (дистрибутив, утилита, плагин немесе веб-плагин);
- Kaspersky бағдарламасының нұсқасы;
- Kaspersky бағдарламасының локализация тілі.

4-қадам. Басқарылатын бағдарламаларға арналған плагиндерді таңдау

Орнату үшін басқарылатын бағдарламалардың плагиндерін таңдаңыз. Kaspersky серверлерінде орналасқан плагиндер тізімі көрсетіледі. Тізім шебердің алдыңғы қадамында таңдалған параметрлерге сәйкес сүзгіленген. Әдепкі бойынша, барлық тілдердің плагиндері толық тізімге енгізілген. Таңдалған тілде тек плагинді көрсету үшін **Басқару консолінің тілін көрсету немесе** ашылмалы тізімінен тілді таңдаңыз. Плагиндер тізімі келесі бағандарды қамтиды:

- **Бағдарлама атауы**

  Қосылатын модульдер, алдыңғы қадамда таңдалған қорғаныс аумақтары мен платформаларына байланысты таңдалды.

- **Бағдарлама нұсқасы**

  Тізімге Kaspersky серверлерінде орналастырылған плагиндердің барлық нұсқалары қосылған. Әдепкі бойынша плагиндердің соңғы нұсқалары таңдалған.

- **Локализация тілі**

  Әдепкі бойынша, плагинді локализациялау тілі, орнату кезінде таңдалған Kaspersky Security Center тіліне байланысты. Басқа тілдерді **Басқару консолінің тілін көрсету немесе** ашылмалы тізімінен таңдауға болады.

Плагиндерді таңдағаннан кейін, оларды орнату автоматты түрде бөлек терезеде басталады. Кейбір плагиндерді орнату үшін сіз Лицензиялық келісімнің шарттарын қабылдауыңыз қажет. Лицензиялық келісімнің мәтінімен танысыңыз, **Лицензиялық келісімнің шарттарын қабылдаймын** параметрін таңдап, **Орнату** түймесін басыңыз. Лицензиялық келісімнің шарттарымен келіспесеңіз, плагин орнатылмайды.

Орнату аяқталғаннан кейін, орнату терезесін жабыңыз.

Сондай-ақ, сіз басқару плагинін бағдарламаны жылдам іске қосу шеберін іске қоспай, кейінірек таңдай аласыз.

5-қадам. Дистрибутивтерді жүктеу және орнату пакеттерін жасау

Kaspersky Endpoint Security for Windows бағдарламасы клиент құрылғыларында сақталатын ақпаратты шифрлау аспаптарын қамтиды. Ұйымыңыздың қажеттіліктері үшін жарамды Kaspersky Endpoint Security for Windows дистрибутивін жүктеп алу үшін ұйымыңыздың клиент құрылғылары орналасқан елдің заңнамасын қараңыз.

Шифрлау түрі терезесінде келесі шифрлау түрлерінің бірін таңдаңыз:

- Күшті шифрлау (AES256). Осы шифрлау түрі үшін 256 разрядты кілт қолданылады.
- Жеңіл шифрлау (AES56). Осы шифрлау түрі үшін 56 разрядты кілт қолданылады.

Шифрлау түрі терезесі, қорғаныс аумағы ретінде **Жұмыс станциялары** нұсқасы, ал платформа ретінде **Microsoft Windows** таңдалса ғана көрсетіледі.

Шифрлау түрін таңдағаннан кейін, шифрлаудың екі түріне де дистрибутивтер тізімі көрсетіледі. Тізімнен таңдалған шифрлау түрі бар дистрибутив таңдалады. Дистрибутив тілі Kaspersky Security Center тіліне сәйкес келеді. Kaspersky Security Center тілі үшін Kaspersky Endpoint Security for Windows дистрибутиві болмаса, ағылшын тіліндегі дистрибутив таңдалады.

Басқару консолінің тілін көрсету немесе ашылмалы тізімінен дистрибутивке арналған тілдерді таңдауға болады.

Басқарылатын бағдарламалардың дистрибутивтері үшін Kaspersky Security Center белгілі бір минималды нұсқасын орнату қажет болуы мүмкін.

Тізімде сіз **Шифрлау түрі** терезесінде таңдалғаннан ерекшеленетін кез келген шифрлау түрінің дистрибутивін таңдай аласыз. Kaspersky Endpoint Security for Windows дистрибутивін таңдағаннан кейін, құрамдастар мен платформаларға сай келетін дистрибутивтерді жүктеу басталады. Жүктеп алудың орындалу барысын **Жүктеп алу күйі** бағанында бақылай аласыз. Бағдарламаны жылдам іске қосу шеберінің жұмысы аяқталғаннан кейін, Windows операциялық жүйесі мен Kaspersky басқарылатын бағдарламалары үшін Желілік агенттің орнату пакеттері **Басқару сервері → Қосымша → Қашықтан орнату → Орнату пакеттері** тізімінде көрсетіледі.

Кейбір дистрибутивтерді жүктеуді аяқтау үшін сіз Лицензиялық келісімді қабылдауыңыз керек. **Қабылдау** түймесін басқан кезде Лицензиялық келісім мәтіні көрсетіледі. Шебердің келесі қадамына өту үшін сіз Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ Kaspersky Құпиялылық саясатының шарттарын қабылдауыңыз керек. Kaspersky Лицензиялық келісімі мен Құпиялылық саясатына қатысты параметрлерді таңдап, Барлығын қабылдау түймесін басыңыз. Егер сіз ережелер мен шарттарды қабылдамасаңыз, пакетті жүктелмейді.

Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ Kaspersky Құпиялылық саясатының шарттарын қабылдағаннан кейін, дистрибутивтерді жүктеу жалғасады. Жүктеу аяқталғаннан кейін, **Орнату пакеті жасалды** күйі көрсетіледі. Болашақта орнату пакеттерін клиент құрылғыларында Kaspersky бағдарламаларын орналастыру үшін пайдалануға болады.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, орнату пакеттерін кейінірек жасауға болады. Басқару консолі тармағында **Басқару сервері → Кеңейтілген → Қашықтан орнату → Орнату пакеттері** бөліміне өтіңіз.

6-қадам. Kaspersky Security Network қолдануды конфигурациялау

Kaspersky бағдарламаларының қауіптерге жауап қайтарудың аса жоғары жылдамдығын қамтамасыз ету үшін Kaspersky Security Network беделдік дерекқорларын қосуға, кейбір қорғаныс құрамдастарының жұмысының тиімділігін арттыруға, сондай-ақ жалған іске қосылу ықтималдығын төмендетуге болады.

Терезеде көрсетілетін KSN мәлімдемесін оқып шығыңыз. Kaspersky Security Center жұмысы туралы ақпаратты Kaspersky Security Network білім базасына беру параметрлерін конфигурациялаңыз. Келесі нұсқалардың бірін таңдаңыз:

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын**

  Kaspersky Security Center және клиент құрылғыларында орнатылған басқарылатын бағдарламалар, олардың жұмысы туралы ақпаратты Kaspersky Security Network қызметіне автоматты режимде жіберетін болады. Kaspersky Security Network-пен ынтымақтастық, вирустар мен қауіптер туралы дерекқорды барынша жылдам жаңартуды қамтамасыз ете отырып, туындаған қауіпсіздік қауіптеріне жауап беру жылдамдығын арттырады.

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдамаймын**

  Kaspersky Security Center және басқарылатын бағдарламалар өз жұмысы туралы ақпаратты Kaspersky Security Network қызметіне жібермейді.

  Осы параметрді таңдасаңыз, Kaspersky Security Network қызметі өшіріледі.

Kaspersky Endpoint Security for Windows плагинін жүктеп алсаңыз, KSN мәлімдемесінің екеуі де көрсетіледі: Kaspersky Security Center үшін KSN мәлімдемесі және Kaspersky Endpoint Security for Windows үшін KSN мәлімдемесі. Плагиндері жүктеп алынған Kaspersky басқа да басқарылатын бағдарламалары үшін KSN мәлімдемелері бөлек терезелерде көрсетіледі және олардың әрбірін бөлек қабылдау (немесе қабылдамау) керек.

Басқару серверінің Kaspersky Security Network (KSN) қызметіне қатынасуын конфигурациялауды одан әрі Басқару консоліндегі Басқару сервері сипаттары терезесінде де орындауға болады.

7-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Басқарылатын құрылғыларда Kaspersky бағдарламалары жұмыс істеген кезде тіркелетін оқиғалар туралы хабарландыру жіберу параметрлерін конфигурациялаңыз. Бұл параметрлер Басқару сервері үшін әдепкі бойынша мәндер ретінде пайдаланылады.

Kaspersky бағдарламаларының туындайтын оқиғалары туралы хабарландырулар таратылымын конфигурациялау үшін келесі параметрлер қолжетімді:

- **Алушылар (электрондық пошта мекенжайлары)**

  Бағдарлама хабарландыру жіберетін пайдаланушылардың электрондық пошта мекенжайлары. Бір не бірнеше мекенжайды енгізуге болады; бірнеше мекенжай енгізілсе, оларды нүктелі үтірмен бөліңіз.

- **SMTP серверлері**

  Ұйымыңыздың пошта серверлерінің мекенжайы немесе мекенжайлары.

  Бірнеше мекенжайды көрсетсеңіз, оларды үтірлі нүктемен бөліңіз. Келесі параметр мәндерін пайдалануыңызға болады:

  - IPv4 мекенжайы немесе IPv6 мекенжайы;
  - Windows желісіндегі құрылғының атауы (NetBIOS атауы);
  - SMTP сервері DNS атауы.

- **SMTP серверінің порты**

  SMTP серверінің коммуникациялық портының нөмірі. Бірнеше SMTP серверін қолдансаңыз, олармен қосылым көрсетілген коммуникациялық порт арқылы орнатылады. Әдепкі бойынша 25-порт орнатылған.

- **ESMTP аутентификациясын пайдалану**

  ESMTP аутентификациясын қолдауды қосу. Жалаушаны қойғаннан кейін, ESMTP аутентификациясы параметрлерін **Пайдаланушы аты** және **Құпиясөз** өрістерінде көрсетуге болады. Әдепкі бойынша, жалауша алынып тасталған.

- **Параметрлер**

  Келесі параметрлерді белгілеңіз:

  - **Тақырып** (электрондық хат тақырыбының атауы).
  - **Электрондық пошта жіберушінің мекенжайы.**
  - **SMTP сервері үшін TLS параметрлері.**

  SMTP сервері үшін TLS параметрлерін көрсетуіңізге болады:

  SMTP сервері осы протоколды қолдайтын болса, TLS қолдануды өшіре аласыз, TLS қолдана аласыз немесе тек TLS-ті күштеп қолдана аласыз. Егер сіз тек TLS пайдалануды ұйғарсаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, тек TLS пайдалануды ұйғарсаңыз, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификат көрсете аласыз.

  - SMTP серверінің сертификаты файлын таңдаңыз:

  Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

  - Клиент сертификаты файлын таңдаңыз:

  Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

  - X.509 сертификаты:

  Сертификаты бар файлды және жеке кілт файлын көрсетіңіз. Сіз бұл файлдарды кез келген ретпен жүктей аласыз. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді енгізіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

  - pkcs12 контейнері:

  Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

Электрондық пошта хабарлары туралы хабарландыру параметрлерін **Тексеру хабарын жіберу** түймесі арқылы тексеруге болады.

Оқиға хабарландыруларын, бағдарламаны жылдам іске қосу шеберін іске қоспай-аяқ, кейінірек конфигурациялай аласыз.

8-қадам. Жаңартуларды басқару параметрлерін конфигурациялау

Клиент құрылғыларында орнатылған бағдарлама жаңартуларымен жұмыс істеу параметрлерін конфигурациялаңыз.

Осалдықтар мен патчтарды басқару мүмкіндіктерін көздейтін лицензиялық кілтті берсеңіз ғана бұл параметрлерді конфигурациялай аласыз.

Жаңартуларды іздеу және орнату режимі параметрлері блогында Kaspersky Security Center жаңартуларын іздеу және орнату режимдерінің бірін таңдай аласыз:

- **Қажетті жаңартуларды іздеу**

  Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бұрын жасалмаған болса, автоматты түрде жасалады.

  Әдепкі бойынша, осы нұсқа таңдалады.

- **Қажетті жаңартуларды іздеу және орнату**

  Осалдықтарды және қажетті жаңартуларды іздеу және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмалары бұған дейін жасалмаған болса, автоматты түрде жасалады.

Windows Server Жаңарту қызметтері параметрлері блогында жаңартуларды синхрондау көзін таңдай аласыз:

- **Домен саясатында белгіленген жаңарту көздерін қолдану**

  Windows Update жаңартулары клиент құрылғыларына домен саясаты параметрлеріне сай жүктеледі. Желілік агент саясаты бұрын жасалмаған болса, автоматты түрде жасалады.

- **Басқару серверін WSUS сервері ретінде пайдалану**

  Windows Update жаңартулары клиент құрылғыларына Басқару серверінен жүктеледі. *Windows Update жаңартуларын синхрондау* тапсырмасы және Желілік агент саясаты бұған дейін жасалмаған болса, автоматты түрде жасалады.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ *Осалдықтарды және қажетті жаңартуларды іздеуді жасауға* және *Қажетті жаңартуларды орнатуға және осалдықтарды түзетуге* болады. Басқару серверін WSUS сервері ретінде қолдану үшін сізге *Windows Update жаңартуларын синхрондау* тапсырмасын жасап, Желілік агент саясатында **Басқару серверін WSUS сервері ретінде пайдалану** параметрін таңдау керек.

9-қадам. Қорғаудың бастапқы конфигурациясын жасау

Қорғаудың бастапқы конфигурациясын жасау терезесінде автоматты түрде жасалған саясаттар мен тапсырмалар тізімі көрсетіледі. Келесі саясаттар мен тапсырмалар құрылады:

- Kaspersky Security Center Желілік агенті саясаты
- Басқару плагиндері бұған дейін орнатылған Kaspersky басқарылатын бағдарламаларына арналған саясаттар

- Басқару серверіне техникалық қызмет көрсету тапсырмасы
- Басқару сервері деректерінің резервтік қоймасы тапсырмасы
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы
- Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы
- Жаңартуды орнату тапсырмасы

Шебердің келесі қадамына өту үшін саясаттар мен тапсырмалардың жасалуының аяқталуын күтіңіз.

Kaspersky Endpoint Security for Windows 10 Service Pack 1 және одан да жоғары нұсқасына арналған 11.0.1 нұсқасына дейінгі плагинді жүктеп, орнатқан болсаңыз, саясаттар мен тапсырмаларды жасау барысында Kaspersky Endpoint Security for Windows сенімді аймағын бастапқы конфигурациялау терезесі ашылады. Бағдарлама кездейсоқ бұғаттауды болдырмау үшін, олардың бағдарламаларын тексеруден шығару үшін Kaspersky тексерген жеткізушілерді сенімді аймаққа енгізуді ұсынады. Консоль ағашында **Саясаттар** → Kaspersky Endpoint Security сипаттары мәзірі → **Кеңейтілген қорғаныс** → **Сенімді аймақ** → **Конфигурациялау** → **Қосу** тармағын таңдап, ұсынылған ерекшеліктерді дәл қазір жасай аласыз немесе ерекшеліктер тізімін кейінірек жасай аласыз. Тексеру ерекшеліктерінің тізімі бағдарламамен әрі қарай жұмыс істеген кез келген уақытта өңдеуге қолжетімді.

> Сенімді аймақпен жұмыс Kaspersky Endpoint Security for Windows бағдарламасының құралдарымен орындалады. Операцияларды орындау бойынша толығырақ нұсқаулар және шифрлау ерекшеліктерінің сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

Сенімді аймақты бастапқы конфигурациялауды аяқтау және шеберге оралу үшін **OK** түймесін басыңыз.

Келесі түймесін басыңыз. Түйме, барлық қажетті саясаттар мен тапсырмалар жасалған кезде қолжетімді болады.

Сондай-ақ, бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қажетті тапсырмалар мен саясаттарды кейінірек жасауға болады.

10-қадам. Ұялы құрылғыларды қосу

Бұған дейін шебердің параметрлерінде **Ұялы құрылғылар** қорғаныс аймағын қосқан болсаңыз, ұйым басқаратын корпоративтік ұялы құрылғыларды қосу параметрлерін көрсетіңіз. **Ұялы құрылғылар** қорғаныс аймағын қоспаған болсаңыз, бұл қадам өткізіп жіберіледі.

Шебердің осы қадамында келесі әрекеттерді орындаңыз:

- Ұялы құрылғыларды қосу порттарын конфигурациялаңыз.
- Басқару серверінің түпнұсқалық растамасы параметрлерін конфигурациялаңыз.
- Сертификаттарды жасаңыз немесе басқарыңыз.
- Жалпы сертификаттарды шығаруды, автоматты түрде жаңартуды және шифрлауды конфигурациялаңыз.
- Ұялы құрылғыларды жылжыту ережелерін жасаңыз.

Ұялы құрылғыларды қосу порттарын конфигурациялау үшін:

1. **Конфигурациялау** өрісінің оң жағындағы **Ұялы құрылғыларды қосу** түймесін басыңыз.
2. Ашылмалы тізімнен **Порттарды теңшеу** тармағын таңдаңыз.

   Қосымша порттар бөлімінде Басқару сервері сипаттары терезесі ашылады.
3. **Қосымша порттар** бөлімінде ұялы құрылғыларды қосу параметрлерін конфигурациялай аласыз:

   - **Белсендіру прокси-серверіне арналған SSL порты**

     Kaspersky Endpoint Security for Windows бағдарламасын Kaspersky белсендіру серверлеріне қосуға арналған SSL порты нөмірі.

     Әдепкі бойынша 17000-порт орнатылған.

   - **Ұялы құрылғыларға арналған портты ашу**

     Ұялы құрылғылар Лицензиялау серверіне қосылатын порт ашылады. Төмендегі өрістерде порт нөмірін және басқа конфигурацияларды белгілеуге болады.

     Әдепкі бойынша, параметр қосулы.

   - **Ұялы құрылғыны синхрондау порты**

     Ұялы құрылғылар Басқару серверіне қосылып, онымен ақпарат алмасатын порт нөмірі. Әдепкі бойынша 13292-порт орнатылған.

     13292-порт қандай да бір басқа мақсаттарда пайдаланылса, басқа портты тағайындауға болады.

   - **Ұялы құрылғыларды белсендіруге арналған порт**

     Kaspersky Endpoint Security for Android қолданбасын Kaspersky белсендіру серверлеріне қосу порттары.

     Әдепкі бойынша 17100-порт орнатылған.

   - **UEFI деңгейлі қорғанысты және KasperskyOS құрылғылары үшін портты ашу**

     UEFI деңгейлі қорғанысты құрылғылар Басқару серверіне қосыла алады.

   - **UEFI деңгейлі қорғанысты және KasperskyOS құрылғыларына арналған порт**

     UEFI деңгейлі қорғанысты және KasperskyOS құрылғылары үшін портты ашу нұсқасы таңдалса, порт нөмірін өзгертуге болады. Әдепкі бойынша 13294-порт орнатылған.

   - **Prometheus арналған ашық порт**

     Prometheus енгізілген өзгерістерін қосу сұрауларының порты. Әдепкі бойынша 13296-порт орнатылған.
4. Өзгерістерді сақтау және бағдарламаны жылдам іске қосу шеберіне оралу үшін **OK** түймесін басыңыз.

Басқару серверінің түпнұсқалық растамасын ұялы құрылғылар тарапынан және ұялы құрылғылардың түпнұсқалық растамасын Басқару сервері тарапынан конфигурациялауыңыз керек болады. Бағдарламаның архитектурасын, бағдарламаны жылдам іске қосу шеберіне қарамастан, кейінірек конфигурациялауға болады.

Басқару серверінің түпнұсқалық растамасы параметрлерін ұялы құрылғылар тарапынан конфигурациялау үшін:

1. **Конфигурациялау** өрісінің оң жағындағы **Ұялы құрылғыларды қосу** түймесін басыңыз.

2. Ашылмалы тізімнен **Түпнұсқалық растаманы теңшеу** тармағын таңдаңыз.

   Сертификаттар бөлімінде Басқару сервері сипаттары терезесі ашылады.

3. **Ұялы құрылғылармен Басқару серверін аутентификациялау** параметрлері тобында ұялы құрылғылар үшін түпнұсқалық растама нұсқасын, ал **UEFI деңгейлі қорғанысты құрылғылармен Басқару серверін аутентификациялау** параметрлері тобында UEFI деңгейлі қорғанысты құрылғылар үшін түпнұсқалық растама нұсқасын таңдаңыз.

   Клиент құрылғыларымен ақпарат алмасу кезінде Басқару серверінің түпнұсқалық растамасы сертификат негізінде жүзеге асырылады.

   Әдепкі бойынша, Басқару серверін орнату кезінде жасалған сертификатты пайдалану таңдалады. Қажет болса, жаңа сертификат қосуға болады.

Жаңа сертификат қосу үшін (міндетті емес):

1. **Басқа сертификат** таңдаңыз.

   Шолу түймесі пайда болады.

2. **Шолу** түймесін басыңыз.

3. Пайда болған терезеде сертификат параметрлерін конфигурациялаңыз:

   - **Сертификат түрі**

     Ашылмалы тізімнен сертификат түрін таңдауға болады:

     - **X.509 сертификаты**. Егер бұл параметр таңдалса, сіз жеке кілтті және жалпыға ортақ сертификатты көрсетуіңіз қажет:

       - **Жабық кілт (.prk, .pem)**. Бұл өрісте PKCS #8 (.prk) пішіміндегі сертификаттың жеке кілтін көрсету үшін **Шолу** түймесін басыңыз.

       - **Жалпыға ортақ кілт (.cer)**. PEM (.cer) пішіміндегі жалпыға ортақ кілтті кілтін көрсету үшін **Шолу** түймесін басыңыз.

     - **PKCS #12 контейнері**. Осы нұсқаны таңдасаңыз, **Шолу** түймесін басу және **Сертификат файлы** өрісін толтыру арқылы P12 немесе PFX пішіміндегі сертификат файлын көрсете аласыз.

   - Белсендіру мерзімі:

     - **Дереу**

       Ағымдағы сертификат **OK** түймесін басқаннан кейін бірден жаңа сертификатпен ауыстырылады.

       Бұған дейін қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды.

     - **Көрсетілген мерзімнен кейін, тәулік**

       Егер бұл нұсқа таңдалса, резервтік сертификат жасалады. Ағымдағы сертификат, көрсетілген күндер санынан кейін жаңа сертификатпен ауыстырылады. Резервтік сертификат күшіне енетін күн **Сертификаттар** бөлімінде көрсетіледі.

Сертификаттарды қайта шығаруды алдын ала жоспарлау ұсынылады. Резервтік сертификат, көрсетілген мерзім аяқталғанға дейін ұялы құрылғыларға жүктелуі керек. Ағымдағы сертификат жаңа сертификатпен ауыстырылғаннан кейін, резервтік сертификаты жоқ, бұрын қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды.

4. Басқару серверінің таңдалған сертификатының параметрлерін көру үшін **Сипаттар** түймесін басуға болады.

Басқару сервері арқылы шығарылған сертификатты қайта шығару үшін:

1. **Сертификат Басқару серверінің құралдары арқылы шығарылған** таңдаңыз.
2. **Қайта шығару** түймесін басыңыз.
3. Ашылған терезеде келесі параметрлерді конфигурациялаңыз:
   - Байланыстың мекенжайы:
     - **Бұрынғы байланыс мекенжайын қалдыру**

       Ұялы құрылғылар қосылатын Басқару серверінің мекенжайы өзгеріссіз қалады.

       Әдепкі бойынша, осы нұсқа таңдалады.

     - **Қосылу мекенжайын мынаған өзгерту**

       Ұялы құрылғыларды басқа мекенжай бойынша қосу қажет болса, өріске қажетті мекенжайды енгізіңіз.

       Ұялы құрылғыларды қосу мекенжайын өзгерткен кезде жаңа сертификат шығару қажет. Ескі сертификат қосылған ұялы құрылғыларда жарамсыз болады. Бұрын қосылған құрылғылар Басқару серверіне қосыла алмайды және бұдан былай оларды басқару мүмкін болмайды.

   - Белсендіру мерзімі:
     - **Дереу**

       Ағымдағы сертификат **OK** түймесін басқаннан кейін бірден жаңа сертификатпен ауыстырылады.

       Бұған дейін қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды.

     - **Көрсетілген мерзімнен кейін, тәулік**

       Егер бұл нұсқа таңдалса, резервтік сертификат жасалады. Ағымдағы сертификат, көрсетілген күндер санынан кейін жаңа сертификатпен ауыстырылады. Резервтік сертификат күшіне енетін күн **Сертификаттар** бөлімінде көрсетіледі.

       Сертификаттарды қайта шығаруды алдын ала жоспарлау ұсынылады. Резервтік сертификат, көрсетілген мерзім аяқталғанға дейін ұялы құрылғыларға жүктелуі керек. Ағымдағы сертификат жаңа сертификатпен ауыстырылғаннан кейін, резервтік сертификаты жоқ, бұрын қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды.

4. Өзгерістерді сақтау және **OK** терезесіне оралу үшін **Сертификаттар** түймесін басыңыз.
5. Өзгерістерді сақтау және бағдарламаны жылдам іске қосу шеберіне оралу үшін **OK** түймесін басыңыз.

Басқару сервері арқылы ұялы құрылғыларды анықтау үшін жалпы сертификаттарды шығаруды, автоматты түрде жаңартуды және шифрлауды конфигурациялау:

1. **Ұялы құрылғы аутентификациясы** өрісінің оң жағындағы **Конфигурациялау** түймесін басыңыз.

   Сертификаттарды шығару ережелері бөлімінде **Ұялы құрылғы сертификаттарын шығару** терезесі ашылады.

2. Қажет болса, **Шығару параметрлері** параметрлері блогында келесі параметрлерді конфигурациялаңыз:

   - **Сертификаттың әрекет ету мерзімі, күндер**

     Сертификаттың күндердегі жарамдылық мерзімі. Әдепкі бойынша, сертификаттың жарамдылық мерзімі 365 күнді құрайды. Осы мерзім өткеннен кейін. ұялы құрылғы Басқару серверіне қосыла алмайды.

   - **Сертификат көзі**

     Ұялы құрылғыларға арналған жалпы сертификаттар көзін таңдау: сертификаттарды Басқару сервері шығарады немесе сертификаттар қолмен беріледі.

     PKI жүйесімен интеграциялау бөлімінде жалпыға ортақ кілт инфрақұрылымымен біріктіру конфигурацияланған болса, сертификат үлгісін өзгертуге болады. Бұл жағдайда, шаблонды таңдаудың келесі өрістері қолжетімді болады:

   - **Әдепкі үлгі**

     Сертификаттардың сыртқы көзі – сертификаттау орталығы шығарған сертификатты әдепкі бойынша белгіленген үлгі бойынша пайдалану.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Басқа үлгі**

     Сертификаттар шығаруға негіз болатын үлгіні таңдау. Сертификат үлгілерін доменде белгілеуге болады. **Тізімді жаңарту** түймесі арқылы сертификаттар үлгілерінің тізімін жаңартуға болады.

3. Қажет болса, **Автоматты жаңартулар параметрлері** параметрлері блогында сертификаттарды автоматты түрде шығарудың келесі параметрлерін белгілеңіз:

   - **Сертификат (күннен) кейін аяқталған кезде келесіні жаңартыңыз**

     Басқару сервері жаңа сертификат шығаруы тиіс ағымдағы сертификаттың жарамдылық мерзімі біткенге дейінгі күндер саны. Мысалы, егер өрісте 4 мәні көрсетілген болса, Басқару сервері ағымдағы сертификаттың жарамдылық мерзімінің бітуіне дейін төрт күн қалғанда жаңа сертификат шығарады. Әдепкі бойынша, 7 мәні көрсетілген.

   - **Мүмкін болса, сертификатты автоматты түрде қайта шығару**

     Сертификатты **Сертификат (күннен) кейін аяқталған кезде келесіні жаңартыңыз** өрісінде көрсетілген жарамдылық мерзімі аяқталғанға дейінгі күн бұрын автоматты түрде қайта шығару үшін осы параметрді таңдаңыз. Егер сертификат қолмен белгіленсе, оны автоматты түрде жаңарту мүмкін емес және қосылған параметр жұмыс істемейді.

     Әдепкі бойынша, параметр өшірулі.

   Сертификаттарды сертификаттау орталығы автоматты түрде жаңартады.

4. Қажет болса, **Құпиясөзбен қорғау** параметрлері блогында орнатылған кезде сертификаттарды шифрсыздау параметрлерін конфигурациялаңыз.

Ұялы құрылғыға сертификат орнатқан кезде пайдаланушыдан құпиясөз сұралуы үшін **Сертификатты орнату кезінде құпиясөзді сұрау** параметрін таңдаңыз. Құпиясөз ұялы құрылғыға сертификат орнатқан кезде, тек бір рет қолданылады.

Құпиясөз Басқару сервері арқылы автоматты түрде жасалады және сіз көрсеткен электрондық пошта мекенжайына жіберіледі. Құпиясөзді пайдаланушыға басқа жолмен бергіңіз келсе, пайдаланушының электрондық пошта мекенжайын немесе өзіңіздің жеке мекенжайыңызды көрсете аласыз.

Жүгірткіні пайдаланып, сертификатты шифрсыздау үшін құпиясөз таңбаларының санын көрсетуге болады.

Құпиясөзді сұрау функциясы, мысалы, Kaspersky Endpoint Security for Android автономды орнату пакетіндегі жалпы сертификатты қорғау үшін қажет. Құпиясөзбен қорғау қаскүнемге Kaspersky Security Center веб-серверінен автономды орнату пакетін ұрлау кезінде жалпы сертификатқа қатынасуға мүмкіндік бермейді.

Егер параметр өшірулі болса, орнату кезінде сертификатты шифрсыздау автоматты түрде жүзеге асырылады және пайдаланушыдан құпиясөз сұралмайды. Әдепкі бойынша, параметр өшірулі.

5. Өзгерістерді сақтау және бағдарламаны жылдам іске қосу шебері терезесіне оралу үшін **OK** түймесін басыңыз.

   Енгізілген өзгерістерді сақтамай, бағдарламаны жылдам іске қосу шеберіне оралу үшін **Бас тарту** түймесін басыңыз.

Ұялы құрылғыларды өзіңізге қажетті басқару тобына жылжыту функциясын қосу үшін,

Ұялы құрылғыларды автоматты түрде жылжыту өрісінде **Ұялы құрылғылар үшін жылжыту ережесін жасау** параметрін таңдаңыз.

Ұялы құрылғылар үшін жылжыту ережесін жасау параметрі таңдалса, бағдарлама Android және iOS операциялық жүйелері басқаратын құрылғыларды **Басқарылатын құрылғылар** тобына көшіретін жылжыту ережесін автоматты түрде жасайды:

- Kaspersky Endpoint Security for Android және ұялы құрылғы сертификаты орнатылған Android операциялық жүйелерімен;
- жалпы сертификаты бар iOS MDM профилі орнатылған iOS операциялық жүйесімен.

Егер мұндай ереже бұрыннан бар болса, онда бағдарлама ереже жасамайды.

Әдепкі бойынша, параметр өшірулі.

Kaspersky бұдан былай Kaspersky Safe Browser-ді қолдамайды.

11-қадам. Жаңартуларды жүктеп алу

Kaspersky Security Center бағдарламасы және Kaspersky басқарылатын бағдарламалары үшін антивирустық дерекқорлардың жаңартулары автоматты түрде жүктеледі. Жаңартулар Kaspersky серверлерінен жүктеледі.

Бағдарламаны жылдам іске қосу шеберін іске қоспай, жаңартуларды жүктеп алу үшін, *Басқару серверінің жаңартулар қоймасына жаңартуларды жүктеу* тапсырмасын жасап, конфигурациялаңыз.

12-қадам. Құрылғыларды табу

Желіде сауалнама өткізу ақпараттық терезесінде Басқару серверінің желіде сауалнама өткізу күйі туралы ақпарат көрсетіледі.

Басқару сервері желіде тапқан құрылғыларды қарап шыға аласыз және терезенің астындағы сілтемелер бойынша **Құрылғыны табу** терезесімен жұмыс істеу бойынша анықтама ала аласыз.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, желіде кейінірек сауалнама өткізуге болады. Windows домендері, Active Directory, IP ауқымдары және IPv6 желілері сауалнамаларын конфигурациялау үшін Басқару консолін пайдаланыңыз.

13-қадам. Бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау

Антивирустық бағдарламаларды және/немесе Желілік агентті желіңіздегі құрылғыларға автоматты түрде орнатқыңыз келсе, бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау терезесінде **Қашықтан орнату шеберін іске қосу** параметрін таңдаңыз.

Шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Басқару консолі мен Басқару серверінің қосылымын конфигурациялау

Басқару консолі Басқару серверіне TCP 13291 SSL порты бойынша қосылған. Дәл осы портты klakaut автоматтандыру нысандары қолдануы мүмкін.

TCP 14000 порты Басқару консолін, тарату нүктелерін, қосалқы Басқару серверлерін және klakaut утилитасының автоматтандыру нысандарын қосу, сондай-ақ клиент құрылғыларынан деректер алу үшін пайдаланылуы мүмкін.

Әдетте, TCP 13000 SSL портын тек Желілік агент, қосалқы Сервер және демилитаризацияланған аймақта орналасқан басты Басқару сервері ғана қолдана алады. Кейбір жағдайларда, Басқару консолін 13000 SSL порты арқылы қосу қажет болуы мүмкін:

- Басқару консолі үшін де, басқа белсенділіктер үшін де бірдей SSL портын қолданған жөн болса (клиент құрылғыларынан деректерді алу, тарату нүктелерін қосу, қосалқы Басқару серверлерін қосу үшін);
- егер klakaut утилитасын автоматтандыру нысаны Басқару серверіне тікелей емес, демилитаризацияланған аймақта орналасқан тарату нүктесі арқылы қосылса.

Басқару консолін 13000 порты бойынша қосуға рұқсат беру үшін:

1. Басқару сервері орнатылған құрылғының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.
2. Келесі бөлімге өтіңіз:
   - 32 разрядты жүйе үшін:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

- 64 разрядты жүйе үшін:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. LP_ConsoleMustUsePort13291 (DWORD) кілтіне 00000000 мәнін белгілеңіз.

   Әдепкі бойынша, бұл кілт үшін 1 мәні көрсетілген.

4. Басқару сервері қызметін қайта іске қосыңыз.

Нәтижесінде, Басқару консолі 13000 портын пайдалану арқылы Басқару серверіне қосыла алады.

Басқару серверінің интернетке қатынасу параметрлерін конфигурациялау

Kaspersky Security Network пайдалану, сондай-ақ Kaspersky Security Center және Kaspersky басқарылатын бағдарламалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.

Басқару серверінің интернетке қатынасу параметрлерін көрсету үшін:

1. Консоль ағашында **Басқару сервері** түйінін таңдаңыз.

2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесінде **Кеңейтілген** → **Интернет желісіне қатынасу параметрлері** бөліміне өтіңіз.

4. Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін таңдаңыз. Параметр таңдалған болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

   - **Мекенжай**

     Kaspersky Security Center-ді интернетке қосу үшін прокси-сервер мекенжайы.

   - **Порт нөмірі**

     Kaspersky Security Center прокси-қосылымы орнатылатын порт нөмірі.

   - **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

     Жергілікті желідегі құрылғыларға қосылған кезде прокси-сервер қолданылмайды.

   - **Прокси-сервердегі түпнұсқалық растама**

     Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

     Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

   - **Пайдаланушы аты**

     Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Сондай-ақ, бағдарламаны жылдам іске қосу шебері арқылы интернетке қатынасуды конфигурациялуға болады.

Автономды құрылғыларды қосу

Бұл бөлімде автономды құрылғыларды Басқару серверіне қалай қосу керектігі сипатталған (яғни, негізгі желіден тыс басқарылатын құрылғылар).

Сценарий: Автономды құрылғыларды қосылым шлюзі арқылы қосу

Бұл сценарийде, негізгі желіден тыс басқарылатын құрылғыларды Басқару серверіне қалай қосу керектігі сипатталған.

Алдын ала талаптар

Сценарийде келесі алдын ала талаптар бар:

- Сіздің ұйымыңыздың желісінде демилитаризацияланған аймақ (DMZ) ұйымдастырылған.
- Kaspersky Security Center Басқару сервері корпоративтік желіде орналастырылған.

Кезеңдер

Бұл сценарий келесі кезеңдерден тұрады:

1. **Демилитаризацияланған аймақта клиент құрылғысын таңдау**

   Бұл құрылғы қосылым шлюзі ретінде пайдаланылады. Таңдалған құрылғы қосылым шлюздерінің талаптарына сай болуы керек.

2. **Желілік агентті қосылым шлюзі ретінде орнату**

   Таңдалған құрылғыға Желілік агентті орнату үшін жергілікті орнатуды пайдалануды ұсынамыз.

   Әдепкі бойынша орнату файлы келесі мекенжай бойынша орналасқан: \\<Сервер атауы>\KLSHARE\PkgInst\NetAgent_<нұсқа нөмірі>.

   Желілік агентті орнату шеберінің **Қосылым шлюзі** терезесінде **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** параметрін таңдаңыз. Бұл режим бір уақытта қосылым шлюзінің рөлін белсендіреді және Желілік агентке Басқару серверіне қосылуды емес, Басқару серверінен қосылуды күтуді бұйырады.

Болмаса желілік агентті Linux құрылғысына орнатып, желілік агентті қосылым шлюзі ретінде жұмыс істейтіндей конфигурациялауға болады, бірақ Linux құрылғыларында жұмыс істейтін желілік агент шектеулерінің тізіміне назар аударыңыз.

3 Қосылым шлюзінің желілік экранында қосылымдарға рұқсат беру

Басқару сервері демилитаризацияланған аймақтағы қосылым шлюзіне қосыла алуы үшін, Басқару сервері мен қосылым шлюзі арасындағы барлық желілік экрандарда 13000 TCP портына қосылуға рұқсат етіңіз.

Егер қосылым шлюзі интернетте нақты IP мекенжайына ие болмаса, бірақ мұның орнына Network Address Translation (бұдан әрі NAT) артында орналасса, NAT арқылы қосылымдарды жіберу ережесін конфигурациялаңыз.

4 Сыртқы құрылғылар үшін басқару тобын құру

Басқарылатын құрылғылар тобы ішінде Топ құрыңыз. Бұл жаңа топта сыртқы басқарылатын құрылғылар болады.

5 Қосылым шлюзін Басқару серверіне қосу

Сіз конфигурациялаған қосылым шлюзі Басқару серверінен қосылымды күтеді. Алайда, Басқару сервері басқарылатын құрылғылар арасында қосылым шлюзі бар құрылғыны атап көрсетпейді. Мұның себебі, қосылым шлюзі Басқару серверімен байланыс орнатуға тырыспады. Сол себепті, Басқару сервері қосылым шлюзіне қосылуды бастау үшін сізге арнайы процедура қажет болады.

Келесі әрекеттерді орындаңыз:

1. Қосылым шлюзін тарату нүктесі ретінде қосыңыз.
2. Қосылым шлюзін **Тағайындалмаған құрылғылар** тобынан сыртқы құрылғылар үшін құрылға топқа жылжытыңыз.

Қосылым шлюзі қосылған және конфигурацияланған.

6 Сыртқы компьютер құрылғыларын басқару серверіне қосу

Әдетте сыртқы компьютер құрылғылары желінің периметрі ішінде жылжытылмайды. Сондықтан, Желілік агентті орнату кезінде оларды қосылым шлюзі арқылы Басқару серверіне қосу үшін конфигурациялау керек.

7 Сыртқы компьютер құрылғыларының жаңартуларын реттеу

Қауіпсіздік қолданбаларының жаңартулары басқару серверінен жүктеп алынатындай конфигурацияланған болса, сыртқы құрылғылар жаңартуларды қосылым шлюзі арқылы жүктеп алады. Мұның екі кемшілігі бар:

- Бұл компанияның интернет-арнасының өткізу қабілеттілігін алатын артық трафик.
- Бұл жаңартуларды алудың ең жылдам тәсілі емес. Сыртқы құрылғылар үшін Kaspersky жаңарту серверлерінен жаңартуларды алу арзан әрі жылдам болуы мүмкін.

Келесі әрекеттерді орындаңыз:

1. Барлық сыртқы құрылғыны бұрын жасалған жеке басқару тобына жылжытыңыз.
2. Жаңарту тапсырмасынан сыртқы құрылғылары бар топты алып тастау.
3. Сыртқы құрылғылары бар топ үшін бөлек жаңарту тапсырмасын жасаңыз.

8. **Ноутбуктерді Басқару серверіне қосу**

   Кейде ноутбуктер желіде, ал басқа уақытта – желіден тыс болады. Тиімді басқару үшін, олардың орналасқан жеріне байланысты Басқару серверіне басқаша қосылуы қажет. Трафикті тиімді пайдалану үшін олар орналасқан жеріне байланысты әртүрлі көздерден жаңартуларды алуы керек.

   Сізге автономды пайдаланушыларға арналған ережелерді конфигурациялау керек: қосылым профильдері және желілік орналасу сипаттамалары. Әрбір ереже ноутбуктер орналасқан жеріне қарай қосылатын Басқару серверінің үлгісін және олар жаңартуларды алуы тиісті Басқару серверінің үлгісін анықтайды.

Сценарий: демилитаризацияланған аймақтағы Басқару сервері арқылы автономды құрылғыларды қосу

Негізгі желіден тыс орналасқан басқарылатын құрылғыларды Басқару серверіне қосқыңыз келсе, оны демилитаризияланған аймақта (DMZ) орналасқан басқарылатын Басқару сервері арқылы орындауға болады.

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Сіздің ұйымыңыздың желісінде демилитаризацияланған аймақ (DMZ) ұйымдастырылған.
- Kaspersky Security Center Басқару сервері ұйымның ішкі желісінде орналастырылған.

Кезеңдер

Бұл сценарий келесі кезеңдерден тұрады:

1. **Демилитаризацияланған аймақта клиент құрылғысын таңдау**

   Демилитаризацияланған аймақта (DMZ) қосалқы Басқару сервері ретінде пайдаланылатын клиент құрылғысын таңдаңыз.

2. **Kaspersky Security Center Басқару серверін орнату.**

   Осы клиент құрылғысына Kaspersky Security Center Басқару серверін орнатыңыз.

3. **Басқару серверлерінің иерархиясын жасау**

   Егер сіз қосалқы Басқару серверін демилитаризацияланған аймаққа орналастырсаңыз, қосалқы Басқару сервері негізгі Басқару серверінен қосылымды қабылдауы керек. Негізгі Сервер 13000-порт арқылы қосалқы Серверге қосылуы үшін жаңа Басқару серверін қосалқы Сервер ретінде қосыңыз. Серверлерді иерархияға біріктіру кезінде екі Сервердің 13291-порты қолжетімді болуы керек. 13291-порт арқылы Басқару консолі Басқару серверіне қосылады.

4. **Автономды басқарылатын құрылғыларды қосалқы Басқару серверіне қосу**

   Автономды құрылғыларды Басқару сервері мен негізгі желіде орналасқан басқарылатын құрылғылар арасында байланыс орнатылатындай демилитаризацияланған аймақтағы Басқару серверіне қосуға болады. Автономды құрылғылар қосылымды 13000 порты арқылы іске қосады.

Автономды құрылғыларды қосу туралы

Әрқашан негізгі желіден тыс кейбір басқарылатын құрылғыларды (мысалы, компанияның аймақтық филиалдарындағы компьютерлер; әртүрлі сату орындарында орнатылған дүңгіршектер, банкоматтар және терминалдар; қызметкерлердің үй кеңселеріндегі компьютерлер) басқару серверіне тікелей қосу мүмкін емес. Кейбір құрылғылар кейде желінің периметрінен асып кетеді (мысалы, аймақтық филиалдарға немесе клиенттің кеңсесіне баратын пайдаланушылардың ноутбуктері).

Сіз әлі де кеңседен тыс құрылғылардың қорғанысын қадағалап, басқаруыңыз керек – олардың қорғаныс күйі туралы өзекті ақпарат алу және олардағы қауіпсіздік бағдарламаларын жаңартып отыру. Бұл, мысалы, мұндай құрылғы негізгі желіден алшақ жерде бұзылатын болса, ол негізгі желіге қосылғаннан кейін бірден қауіп тарататын платформаға айналуы мүмкін болғандықтан қажет. Автономды құрылғыларды Басқару серверіне қосу үшін келесі екі тәсілді қолдануға болады:

- Демилитаризацияланған аймақтағы (DMZ) қосылымдар шлюзі

  Деректер трафигі схемасын қараңыз: Жергілікті желі (LAN) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар; қосылым шлюзін қолдану.

- Демилитаризацияланған аймақтағы (DMZ) Басқару сервері

  Деректер трафигі схемасын қараңыз: Демилитаризацияланған аймақтың (DMZ) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар.

Демилитаризацияланған аймақтағы қосылымдар шлюзі

Автономды құрылғыларды Басқару серверіне қосудың ұсынылған тәсілі – ұйым желісінде демилитаризацияланған аймақты құру және демилитаризацияланған аймақта қосылым шлюзін орнату. Сыртқы құрылғылар қосылым шлюзіне қосылады, ал желі ішіндегі Басқару сервері құрылғыларға қосылым шлюзі арқылы қосылымды бастайды.

Басқасымен салыстырғанда, бұл ең қауіпсіз болып есептеледі:

- Басқару серверіне сырттан қатынасуды ашудың қажеті жоқ.

- Бұзылған қосылым шлюзі желілік құрылғылардың қауіпсіздігіне үлкен қауіп төндірмейді. Қосылым шлюзі ештеңені басқармайды немесе ешқандай қосылымды орнатпайды.

Бұдан бөлек, қосылым шлюзі көп аппараттық ресурсты қажет етпейді.

Алайда, бұл тәсіл аса күрделі конфигурациялау процесіне ие:

- Құрылғы демилитаризацияланған аймақта қосылым шлюзі рөлін атқаруы үшін сізге Желілік агент орнатып, оны Басқару серверіне ерекше түрде қосу керек.

- Жағдайлар үшін Басқару серверіне бірдей қосылым мекенжайын пайдалана алмайсыз. Периметрдің сыртында сізге басқа мекенжайды (қосылым шлюзінің мекенжайын) ғана емес, сонымен қатар басқа қосылым режимін де қолдану қажет болады: қосылым шлюзі арқылы.

- Сондай-ақ, әртүрлі орындардағы ноутбуктер үшін әртүрлі қосылым параметрлерін анықтау қажет.

Бұрын конфигурацияланған желіге қосылым шлюзін қосу үшін:

1. Желілік агентті қосылым шлюзі режимінде орнатыңыз.

2. Жаңадан қосылған қосылым шлюзіне қосқыңыз келетін құрылғыларда Желілік агентті қайта орнатыңыз.

Демилитаризацияланған аймақтағы (DMZ) Басқару сервері

Тағы бір тәсіл – демилитаризацияланған аймақта бірыңғай Басқару серверін орнату.

Бұл конфигурацияның қауіпсіздігі, бірінші тәсілдің конфигурациясына қарағанда төмен. Бұл жағдайда, сыртқы ноутбуктерді басқару үшін Басқару сервері интернеттен кез келген мекенжайдан қосылымдарды қабылдауы керек. Басқару сервері ішкі желідегі барлық құрылғыларды тек демилитаризацияланған аймақтан басқарады. Сондықтан, мұндай оқиғаның ықтималдығы төмен болғанына қарамастан, бұзылған Сервер үлкен зиян келтіруі мүмкін.

Демилитаризацияланған аймақтағы Басқару сервері ішкі желі құрылғыларын басқара алмаса, қауіп айтарлықтай төмендейді. Мұндай конфигурацияны, мысалы, провайдер клиенттердің құрылғыларын басқару үшін қолдана алады.

Бұл тәсілді келесі жағдайларда қолдануға болады:

- Басқару серверін орнатумен және конфигурациялаумен таныс болсаңыз және қосылым шлюзін орнату мен конфигурациялаудың басқа процедурасын орындағыңыз келмесе.

- Егер сізге көптеген құрылғыларды басқару қажет болса. Басқару сервері басқара алатын құрылғылардың ең көп саны – 100 000 құрылғы, қосылым шлюзі 10 000 құрылғыға дейін қолдау көрсете алады.

Бұл шешімнің кейбір қиындықтары да бар:

- Басқару сервері көбірек аппараттық ресурстарды және басқа дерекқорды қажет етеді.

- Құрылғылар туралы ақпарат байланысты емес екі дерекқорда сақталады (желі ішіндегі Басқару сервері үшін және екіншісі демилитаризацияланған аймақта), бұл болса бақылауды қиындатады.

- Барлық құрылғыларды басқару үшін Басқару сервері иерархияға біріктірілуі керек, бұл болса бақылау мен басқаруды қиындатады. Қосалқы Басқару серверінің үлгісі басқару топтарының ықтимал құрылымдарына шектеулер қояды. Қосалқы басқару серверіне қандай тапсырмалар мен саясаттарды және қалай кеңейту керектігін шешуіңіз керек.

- Сыртқы құрылғыларды демилитаризацияланған аймақта Басқару сервері пайдалану үшін және негізгі Басқару серверін ішкі жағынан пайдалану үшін конфигурациялау шлюз арқылы қосылымды конфигурациялаудан оңай емес.

- Қауіпсіздіктің жоғары тәуекелдері. Бұзылған Басқару сервері басқарылатын ноутбуктерді бұзуды жеңілдетеді. Егер бұл орын алса, хакерлер жергілікті желіге шабуылды жалғастыру үшін ноутбуктердің біреуі корпоративті желіге оралғанша күтуі керек.

Сыртқы компьютер құрылғыларын басқару серверіне қосу

Әрқашан негізгі желіден тыс компьютер құрылғыларын (мысалы, компанияның аймақтық филиалдарындағы компьютерлер; әртүрлі сату орындарында орнатылған дүңгіршектер, банкоматтар және терминалдар; қызметкерлердің үй кеңселеріндегі компьютерлер) басқару серверіне тікелей қосу мүмкін емес. Олар Басқару серверіне демилитаризацияланған аймақта (DMZ) орнатылған қосылым шлюзі арқылы қосылуы керек. Бұл конфигурация осы құрылғыларға желілік агент орнатылған кезде орындалады.

Сыртқы компьютер құрылғыларын басқару серверіне қосу үшін:

1. Желілік агенттің орнату пакетін жасау.
2. Жасалған орнату пакетінің сипаттарын ашыңыз, **Қосымша** бөліміне өтіңіз және **Басқару серверіне байланыс шлюзі арқылы қосылу** параметрін ашыңыз.

   Басқару серверіне байланыс шлюзі арқылы қосылу параметрі **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** параметрімен үйлеспейді. Сіз бұл параметрлердің екеуін де бір уақытта қоса алмайсыз.

3. **Қосылым шлюзі мекенжайы** өрісінде қосылым шлюзі мекенжайын көрсетіңіз.

   Егер қосылым шлюзі Network Address Translation (NAT) артында орналасқан болса және өзінің жалпыға ортақ мекенжайы болмаса, қосылымдарды жалпыға ортақ мекенжайдан қосылым шлюзінің ішкі мекенжайына бағыттау үшін NAT шлюз ережесін конфигурациялаңыз.

4. Жасалған орнату пакеті негізінде Жеке орнату пакетін жасаңыз.
5. Жеке орнату пакетін мақсатты құрылғыларға электронды түрде немесе алынбалы жетекте жеткізіңіз.
6. Жеке орнату пакетіндегі Желілік агентті орнатыңыз.

Басқару серверіне сыртқы компьютер құрылғылары қосылған.

Автономды пайдаланушыларға арналған қосылым профильдері туралы

Ноутбуктерді (бұдан әрі - "құрылғылар") пайдаланатын автономды пайдаланушылар жұмыс істеген кезде, құрылғының желідегі ағымдағы жайғасымына байланысты Басқару серверіне қосылу тәсілін өзгерту немесе Басқару серверлері арасында ауысу қажет болуы мүмкін.

Қосылым профильдеріне тек Windows және macOS басқаратын құрылғылар үшін ғана қолдау көрсетіледі.

Бір Басқару серверінің әртүрлі мекенжайларын пайдалану

Желілік агенті орнатылған құрылғылар әртүрлі уақыт аралығында ұйымның ішкі желісінен де, интернеттен де Басқару серверіне де қосыла алады. Бұл жағдайда, Желілік агент Басқару серверіне қосылу үшін әртүрлі мекенжайларды қолдануы қажет болуы мүмкін: интернеттен қосылған кезде Сервердің сыртқы мекенжайы және ішкі желіден қосылған кезде Сервердің ішкі мекенжайы.

Бұл үшін, Желілік агент саясатының сипаттарында интернеттен Басқару серверіне қосылу үшін профиль қосыңыз. Саясат сипаттары, **Байланыстардың профильдері** салынған бөлімінде профильді қосыңыз (**Қосылымдар** бөлімі). Профиль жасау терезесінде **Тек жаңартуларды алу үшін пайдалану** параметрін өшіріп, **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау** параметрін таңдау керек. Егер қосылым шлюзі Басқару серверіне қатынасу үшін пайдаланылса (мысалы, Интернеттен қатынасу: Желілік агент демилитаризацияланған аймақтағы қосылым шлюзі ретінде бөлімінде сипатталған Kaspersky Security Center конфигурациясында), қосылым профилінде тиісті өрістегі қосылым шлюзінің мекенжайы көрсетілуі керек.

Ағымдағы желіге байланысты Басқару серверлері арасында ауысу

Егер ұйымда әртүрлі Басқару серверлері бар бірнеше кеңселер болса және олардың арасында Желілік агенті орнатылған құрылғылардың бір бөлігі жылжытылса, онда Желілік агент құрылғы орналасқан кеңсенің жергілікті желісін Басқару серверіне қосылуы керек.

Бұл жағдайда, Желілік агент саясатының сипаттарында бастапқы үйдегі Басқару сервері орналасқан үйдегі кеңсені қоспағанда, әрбір кеңсе үшін Басқару серверіне қосылу профилін жасау керек. Байланыс профильдерінде тиісті Басқару серверлерінің мекенжайларын көрсетіп, **Тек жаңартуларды алу үшін пайдалану** параметрін таңдаңыз немесе өшіріңіз:

- Желілік агент үйдегі Басқару серверімен синхрондауды қажет етсе, ал жергілікті Сервер тек жаңартуларды жүктеу үшін пайдаланылса, параметрді таңдаңыз;
- Желілік агент жергілікті Басқару сервері тарапынан толығымен басқарылуы қажет болса, параметрді өшіріңіз.

Әрі қарай, сіз жасалған профильдерге ауысу шарттарын конфигурациялауыңыз керек: "үйдегі кеңсені" қоспағанда, кеңселердің әрқайсысы үшін кемінде бір шарт. Мұндай шарттардың әрқайсысының мәні кеңселердің біріне тән бөлшектерді желілік ортада табуға негізделеді. Егер шарт шындыққа айналса, тиісті профиль белсендіріледі. Егер шарттардың ешқайсысы дұрыс болмаса, Желілік агент үйдегі Басқару серверіне ауысады.

Автономды пайдаланушылар үшін қосылым профилін жасау

Желілік агент профилін Басқару серверіне қосу тек Windows және macOS операциялық жүйесі басқаратын құрылғылар үшін ғана қолжетімді.

Желілік агентті автономды пайдаланушыларға арналған Басқару серверіне қосу профилін жасау үшін:

1. Консоль ағашында, Серверге Желілік агентті қосу профилін жасау қажет болған клиент құрылғылары үшін басқару тобын таңдаңыз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Топтың барлық құрылғылары үшін қосылым профилін жасағыңыз келсе, **Саясаттар** қойыншасындағы топтың жұмыс аймағында Желілік агенттің саясатын таңдаңыз. Таңдалған саясат сипаттары терезесін ашыңыз.

   - Топтың құрамында таңдалған құрылғы үшін қосылым профилін жасағыңыз келсе, **Құрылғылар** қойыншасындағы топтың жұмыс аймағында құрылғыны таңдап, келесі әрекеттерді орындаңыз:

     a. Таңдалған құрылғы сипаттары терезесін ашыңыз.

     b. Құрылғы сипаттары терезесінің **Бағдарламалар** бөлімінде Желілік агентті таңдаңыз.

     c. Желілік агент сипаттары терезесін ашыңыз.

3. **Қосылым мүмкіндігі** бөлімі сипаттары терезесінде **Байланыс профильдері** салынған бөлімін таңдаңыз.

4. **Басқару серверіне қосылу профильдері** блогында **Қосу** түймесін басыңыз.

   Әдепкі бойынша, қосылым профильдері тізімі <Офлайн-режим> және <Үйдегі Басқару сервері> профильдерін қамтиды. Профильдер өзгерту және жою үшін қолжетімді емес.

   <Офлайн-режим> профилінде қосылуға арналған Сервер көрсетілмейді. Осы профильге өту кезінде, Желілік агент қандай да бір Серверге қосылуға тырыспайды, ал клиент құрылғыларында орнатылған бағдарламалар болса автономды пайдаланушыларға арналған саясаттарды қолданады. <Офлайн-режим> профилі құрылғыны желіден ажырату шарттарында қолданылады.

   <Үйдегі Басқару сервері> профилінде, Желілік агентті орнату кезінде белгіленген қосылуға арналған Сервер көрсетілген. <Үйдегі Басқару сервері> профилі, басқа желіде жұмыс істеген құрылғы қайтадан үйдегі Басқару серверіне қосылатын шарттарда қолданылады.

5. Ашылған **Жаңа профиль** терезесінде қосылым профилінің параметрлерін конфигурациялаңыз:

   - **Профиль атауы**

     Енгізу өрісінде қосылым профилінің атауын қарауға немесе өзгертуге болады.

   - **Басқару сервері**

     Профильді белсендіру кезінде клиент құрылғысы қосылуы тиісті Басқару серверінің мекенжайы.

   - **Порт**

     Қосылым орындалатын порт нөмірі.

   - **SSL порты**

     SSL протоколының көмегімен қосылым орындалатын порт нөмірі.

   - **SSL пайдалану**

     Бұл параметр қосулы болса, қосылым қорғалған порт арқылы орындалатын болады (SSL протоколының көмегімен).

Әдепкі бойынша, параметр қосулы. Сіздің қосылымыңыз қауіпсіз болып қала беруі үшін, бұл параметрді өшірмеу ұсынылады.

- **Прокси-сервер арқылы қосылымды конфигурациялау** сілтемесі бойынша прокси-сервер арқылы қосу профильдерін конфигурациялаңыз. Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін таңдаңыз. Параметр таңдалған болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

  - **Прокси-сервердің мекенжайы**

    Kaspersky Security Center-ді интернетке қосу үшін прокси-сервер мекенжайы.

  - **Порт нөмірі**

    Kaspersky Security Center прокси-қосылымы орнатылатын порт нөмірі.

  - **Прокси-сервердегі түпнұсқалық растама**

    Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

    Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

  - **Пайдаланушы аты** (**Прокси-сервердегі түпнұсқалық растама** параметрі таңдалған болса, өріс қолжетімді болады)

    Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

  - **Құпиясөз** (**Прокси-сервердегі түпнұсқалық растама** параметрі таңдалған болса, өріс қолжетімді болады)

    Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

    Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

- **Қосылым шлюзінің параметрлері**

  Клиент құрылғыларын Басқару серверіне қосатын шлюз мекенжайы.

- **Автономды пайдаланушы режимін қосу**

  Параметр қосулы болса, осы профиль арқылы қосылу кезінде, клиент бағдарламасында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясат профильдерін және автономды пайдаланушыларға арналған саясаттарды қолданатын болады. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, бағдарламалар белсенді саясаттарды қолданатын болады.

  Әдепкі бойынша, параметр өшірулі.

- **Тек жаңартуларды алу үшін пайдалану**

  Бұл параметр қосулы болса, профиль клиент құрылғысында орнатылған бағдарламалар жаңартуларды жүктеп алған кезде ғана қолданылатын болады. Қалған операциялар үшін Басқару серверіне қосылу Желілік агентті орнату кезінде белгіленген бастапқы қосылу параметрлерімен орындалатын болады.

  Әдепкі бойынша, параметр қосулы.

- **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау**

  Бұл параметр қосулы болса, Желілік агент профильдің сипаттарында көрсетілген параметрлерді қолдана отырып, Басқару серверіне қосылады.

  Бұл параметр өшірулі болса, Желілік агент орнату кезінде көрсетілген бастапқы параметрлерді қолдана отырып, Серверге қосылады.

  Тек жаңартуларды алу үшін пайдалану параметрі өшірулі болса, параметр қолжетімді болады.

  Әдепкі бойынша, параметр өшірулі.

6. Қосылу кезінде клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясаттардың профильдерін және Басқару сервері қолжетімді болмаса, автономды пайдаланушыларға арналған саясаттардың профильдерін қолдануы үшін **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу** параметрін таңдаңыз. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

Нәтижесінде, Желілік агентті автономды пайдаланушыларға арналған Басқару серверіне қосу профилі жасалады. Желілік агентті осы профиль арқылы Серверге қосқан кезде, клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясаттарды немесе автономды пайдаланушыларға арналған саясаттарды қолданатын болады.

Желілік агентті басқа Басқару серверіне ауыстырып қосу туралы

Желілік агентті Серверге қосудың бастапқы параметрлері Желілік агентті орнату кезінде белгіленеді. Желілік агентті басқа Басқару серверлеріне ауыстырып қосу үшін ауыстырып қосу ережелерін қолдануға болады. Бұл функцияға тек Windows немесе macOS басқаратын құрылғыларға орнатылған Желілік агенттер үшін қолдау көрсетіледі.

Ауыстырып қосу ережелері келесі желі параметрлері өзгертілгенде іске қосылуы мүмкін:

- Әдепкі қосылым шлюзінің мекенжайы.
- Желідегі DHCP (Dynamic Host Configuration Protocol) серверінің IP мекенжайы.
- Ішкі желінің DNS суффиксі.
- Желідегі DNS серверінің IP мекенжайы.
- Windows доменінің қолжетімділігі. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.
- Мекенжай және ішкі желі маскасы.
- Желідегі WINS серверінің IP мекенжайы. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.
- Клиент құрылғысының DNS атауы немесе NetBIOS атауы.
- SSL қосылым мекенжайының қолжетімділігі.

Желілік агентті басқа Басқару серверлеріне ауыстырып қосу ережелері қалыптастырылған болса, Агент желі параметрлерінің өзгертілуіне келесідей жауап қайтарады:

- Егер желінің сипаттамалары қалыптастырылған ережелердің ешбіріне сай келмесе, онда Желілік агент осы ережеде көрсетілген Басқару серверіне қосылады. Бұл ережемен белгіленген болса, клиент құрылғыларына орнатылған бағдарламалар автономды пайдаланушыларға арналған саясаттарға өтеді.
- Ережелердің ешбірі орындалмай жатса, онда Желілік агент орнату кезінде белгіленген Басқару серверіне қосылу бастапқы параметрлеріне қайта оралады. Клиент құрылғыларында орнатылған бағдарламалар белсенді саясаттарға қайта оралады.
- Басқару сервері қолжетімді болмаса, онда Желілік агент автономды пайдаланушыларға арналған саясаттарды қолданады.

Желілік агент, **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу** параметрі Желілік агент саясатының параметрлерінде қосылған болса ғана автономды пайдаланушыларға арналған саясатқа ауысып қосылады.

Желілік агентті Басқару серверіне қосу параметрлері қосылым профилінде сақталады. Қосылым профилінде сіз клиент құрылғыларын автономды пайдаланушыларға арналған саясаттарға көшіру ережелерін жасай аласыз, сондай-ақ профильді жаңартуларды жүктеп алу үшін қолданылатындай етіп конфигурациялай аласыз.

Желілік агентті желілік орналасу бойынша ауыстырып қосу ережесін жасау

Желілік агентті ауыстырып қосу тек Windows және macOS операциялық жүйесі басқаратын құрылғылар үшін ғана қолжетімді.

Желінің сипаттамаларын өзгерту кезінде Желілік агентті бір Басқару серверінен басқасына ауыстырып қосуға арналған ережені жасау үшін:

1. Консоль ағашында, Желілік агентті желілік орналасу сипаттамасы бойынша ауыстырып қосу ережесін жасауды қажет ететін құрылғылары бар басқару тобын таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:
   - Топтың барлық құрылғылары үшін ережені жасағыңыз келсе, **Саясаттар** қойыншасындағы топтың жұмыс аймағында Желілік агенттің саясатын таңдаңыз. Таңдалған саясат сипаттары терезесін ашыңыз.
   - Топтың таңдалған құрылғысы үшін ережені жасағыңыз келсе, **Құрылғылар** қойыншасындағы топтың жұмыс аймағында құрылғыны таңдап, келесі әрекеттерді орындаңыз:
     a. Таңдалған құрылғы сипаттары терезесін ашыңыз.
     b. Құрылғы сипаттары терезесінің **Бағдарламалар** бөлімінде Желілік агентті таңдаңыз.
     c. Желілік агент сипаттары терезесін ашыңыз.
3. **Қосылым мүмкіндігі** бөлімінде ашылған **Сипаттар** терезесінде **Байланыс профильдері** салынған бөлімін таңдаңыз.

4. **Желілік орналасудың параметрлері** бөлімінде **Қосу** түймесін басыңыз.

5. Ашылған **Жаңа сипаттама** терезесінде желілік орналасудың сипаттамасы параметрлерін және ауыстырып қосу ережелерін конфигурациялаңыз. Желілік орналасудың сипаттамасының келесі параметрлерін конфигурациялаңыз:

   - **Желілік орналасудың сипаттамасының атауы**

     Желілік орналасудың сипаттамасының атауы 255 таңбадан артық болуы және арнайы таңбаларды ("*<>? \/:|) қамтуы мүмкін емес.

   - **Қосылу профилін пайдалану**

     Ашылатын тізімнен Желілік агентті Басқару серверіне қосу профилін таңдауға болады. Профиль желілік орналасудың сипаттамасының шарттарын орындау кезінде қолданылады. Қосылым профилі, Желілік агентті Басқару серверіне қосу параметрлерін қамтиды және клиент құрылғыларын автономды пайдаланушыларға арналған саясаттарға көшіруді айқындайды. Профиль тек жаңартуларды жүктеу үшін ғана қолданылады.

6. Желілік орналасудың сипаттамасы шарттарының тізімін құрастыру үшін **Ауысу шарты** блогында **Қосу** түймесін басыңыз.

   Ереженің шарттары AND логикалық операторын қолданумен бірге біріктіріледі. Желілік орналасудың сипаттамасы бойынша ауысу ережесі іске қосылуы үшін, ереженің барлық ауысу шарттары орындалуы тиіс.

7. Ашылатын тізімнен клиент құрылғысы қосылған желінің сипаттамаларын өзгертуге сай келетін мәнді таңдаңыз:

   - **Әдепкі қосылым шлюзінің мекенжайы** – желінің негізгі шлюзін өзгерту.
   - **DHCP серверінің мекенжайы** – желідегі DHCP (Dynamic Host Configuration Protocol) серверінің IP мекенжайын өзгерту.
   - **DNS домені** – ішкі желінің DNS суффиксін өзгерту.
   - **DNS серверінің мекенжайы** – желідегі DNS серверінің IP мекенжайын өзгерту.
   - **Windows доменінің қолжетімділігі (тек Windows)** – клиент құрылғысы қосылып тұрған Windows доменінің күйін өзгерту. Бұл параметрді Windows басқаратын құрылғылар үшін ғана қолданыңыз.
   - **Ішкі желі** – ішкі желі маскасы мен мекенжайын өзгерту.
   - **WINS серверінің мекенжайы (тек Windows)** – желінің WINS серверінің IP мекенжайын өзгерту. Бұл параметрді Windows басқаратын құрылғылар үшін ғана қолданыңыз.
   - **Атауларды анықтау мүмкіндігі** – клиент құрылғысында NetBIOS атауы немесе DNS атауы өзгерді.
   - **SSL қосылым мекенжайының қолжетімділігі** – клиент құрылғысы берілген сервермен (атауы:порты) SSL қосылымын орната алады немесе орната алмайды (сіз таңдаған опцияға байланысты). Әрбір Сервер үшін сіз SSL сертификатын қосымша түрде көрсете аласыз. Бұл жағдайда желілік агент SSL қосылымының мүмкіндігін тексерумен қатар, басқару серверінің сертификатын тексереді. Сертификаттар сай келмесе, қосылым орнатылмайды. Қосылым жиілігі — минутына бір рет.

8. Ашылған терезеде Желілік агентті басқа Басқару серверіне ауыстырып қосу шартының мәнін көрсетіңіз. Терезенің атауы алдыңғы қадамда мәнді таңдауға байланысты болады. Ауысу шартының келесі параметрлерін конфигурациялаңыз:

   - **Мән**

     Өрісте, жасалатын шарт үшін бір немесе бірнеше мәнді қосуға болады.

   - **Тізімнің кемінде бір мәніне сәйкес болса**

     Осы нұсқа таңдалған болса, шарт **Мән** тізімінде көрсетілген мәндердің кез келгенінде орындалатын болады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Тізім мәндерінің ешқайсысына сәйкес болмаса**

     Осы нұсқа таңдалған болса, шарт, оның мәні **Мән** тізімінде болмаған жағдайда орындалады.

9. Жаңа желілік орналасудың сипаттамасын қолдануды қосу үшін **Жаңа сипаттама** терезесінде **Сипаттама белсенді** параметрін таңдаңыз.

Нәтижесінде, желілік орналасудың сипаттамасы бойынша ауыстырып қосу ережесі жасалып, оның шарттарын орындау кезінде Желілік агент Басқару серверіне қосылу үшін сипаттамада көрсетілген қосылым профилін қолданатын болады.

Желілік орналасудың сипаттамалары, тізімде ұсынылған тәртіп бойынша желінің сипаттамаларына сәйкестік тұрғысынан тексеріледі. Желінің сипаттамалары бірнеше сипаттамаға сай келсе, олардың біріншісі қолданылады. Ережелердің тізімдегі орналасу тәртібін **Жоғары** (⬆) және **Төмен** (⬇) түймелерінің көмегімен өзгерте аласыз.

Оқиға хабарландырулары

Бұл бөлімде клиент құрылғыларындағы оқиғалар туралы әкімшіге хабарлау әдісін қалай таңдауға болатындығы, сондай-ақ оқиғалар туралы хабарлау параметрлерін қалай конфигурациялау керектігі сипатталған.

Сонымен қатар, Eicar сынақ "вирусын" пайдаланып оқиға хабарландыруларының таралуын қалай тексеруге болатыны сипатталған.

Оқиға хабарландырулары параметрлерін конфигурациялау

Kaspersky Security Center бағдарламасы клиент құрылғыларындағы оқиғалар туралы әкімшіге хабарлау тәсілін таңдауға және хабарландыру параметрлерін конфигурациялауға мүмкіндік береді:

- Электрондық пошта. Оқиға орын алған кезде, бағдарлама көрсетілген электрондық пошта мекенжайларына хабарландыру жібереді. Хабарландыру хабарын конфигурациялай аласыз.
- SMS. Оқиға орын алған кезде, бағдарлама көрсетілген телефон нөмірлеріне хабарландырулар жібереді. Пошта шлюзі арқылы SMS хабарландыруларын жіберуді конфигурациялауға болады.
- Орындалатын файл. Құрылғыда оқиға болған кезде орындалатын файл әкімшінің жұмыс станциясында іске қосылады. Орындалатын файлдың көмегімен әкімші болған оқиғаның параметрлерін ала алады.

Клиент құрылғыларындағы оқиғалар туралы хабарландыру параметрлерін конфигурациялау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.

2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.

3. **Хабарландырулар мен оқиғаларды экспорттау параметрлерін конфигурациялау** сілтемесі арқылы өтіп, ашылатын тізімнен **Хабарландыруларды конфигурациялау** мәнін таңдаңыз.

   Сипаттар: Оқиғалар терезесі ашылады.

4. **Хабарландыру** бөлімінде хабарландыру тәсілін таңдаңыз (электрондық пошта, SMS, іске қосылатын орындалатын файл) және хабарландыру параметрлерін конфигурациялаңыз:

   - **Электрондық пошта**

     Электрондық пошта қойындысы оқиғаларға арналған электрондық хат хабарландыруларын конфигурациялауға мүмкіндік береді.

     Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады.

     SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

     - IPv4 мекенжайы немесе IPv6 мекенжайы;
     - Windows желісіндегі құрылғының атауы (NetBIOS атауы);
     - SMTP сервері DNS атауы.

     SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

     DNS MX іздеуін пайдалану параметрін қоссаңыз, SMTP серверінің бірдей DNS атауы үшін IP мекенжайының бірнеше MX жазбасын қолдана аласыз. Бір DNS атауында, алынған электрондық пошталардың әртүрлі басымдықтары бар бірнеше MX жазбалары болуы мүмкін. Басқару сервері MX жазбаларының басымдылығының өсуі ретімен SMTP серверіне электрондық пошта бойынша хабарландырулар жіберуге тырысады. Әдепкі бойынша, параметр өшірулі.

     > **DNS MX іздеуін пайдалану** параметрін қосып, TLS параметрін қолдануға рұқсат бермесеңіз, онда хабарландыруларды электрондық пошта бойынша жіберу кезінде қосымша қорғаныс шарасы ретінде сіздің серверлік құрылғыңызда DNSSEC параметрлерін қолдану ұсынылады.

     Қосымша параметрлерді белгілеу үшін **Параметрлер** сілтемесінен өтіңіз:

     - Тақырып (электрондық пошта тақырыбының атауы).
     - Электрондық пошта жіберушінің мекенжайы.
     - ESMTP аутентификациясы параметрлері.

     SMTP сервері үшін ESMTP аутентификациясы параметрі қосылған болса, SMTP серверінде түпнұсқалық растама үшін есептік жазбаны көрсету керек.

     - SMTP сервері үшін TLS параметрлері:
       - **TLS қолданбау**

Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

- **SMTP сервері қолдаса, TLS қолдану**

SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

- **Әрқашан TLS пайдалану, Сервер сертификатының жарамдылық мерзімін тексеру**

TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

Әрқашан TLS пайдалану, Сервер сертификатының жарамдылық мерзімін тексеру үшін мәнін қолдануды ұйғарсаңыз, сіз SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

SMTP сервері үшін TLS параметрлерін көрсетуіңізге болады:

- SMTP серверінің сертификаты файлын таңдаңыз:

Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

- Клиент сертификаты файлын таңдаңыз:

Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

- X.509 сертификаты:

Сертификаты бар файлды және жеке кілт файлын көрсетуіңіз қажет. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- pkcs12 контейнері:

Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

Хабарландыру хабары өрісінде, оқиға туындаған кезде бағдарлама жіберетін оқиға туралы хабарландырудың стандартты мәтіні қамтылған. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер бар. Хабар мәтінін, оқиғаның егжей-тегжейлі деректері бар жаңа алмастырылатын параметрлерді қосу арқылы өзгертуге болады. Алмастырылатын параметрлер тізімі өрістің оң жағындағы түймені басу арқылы қолжетімді.

Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Хабарлардың дұрыс конфигурацияланғанын тексеру үшін **Тексеру хабарын жіберу** түймесін басыңыз. Бағдарлама көрсетілген электрондық пошта мекенжайларына мәтіндік хабарлар жібереді.

- SMS

SMS қойыншасында ұялы телефонға түрлі оқиғалар туралы SMS хабарландыруларын жіберуді конфигурациялауға болады. SMS хабарлар пошта шлюзі арқылы жіберіледі.

Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады. Хабарландырулар, көрсетілген электрондық пошта мекенжайларымен байланысты нөмірлері бар телефондарға жеткізіледі.

SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

- IPv4 мекенжайы немесе IPv6 мекенжайы;
- Windows желісіндегі құрылғының атауы (NetBIOS атауы);
- SMTP сервері DNS атауы.

SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

Қосымша параметрлерді белгілеу үшін **Параметрлер** сілтемесінен өтіңіз:

- Тақырып (электрондық пошта тақырыбының атауы).
- Электрондық пошта жіберушінің мекенжайы.
- ESMTP аутентификациясы параметрлері.

Қажет болса, SMTP сервері үшін ESMTP аутентификациясы параметрі қосылған болса, SMTP серверінде түпнұсқалық растама үшін есептік жазбаны көрсетуге болады.

- SMTP сервері үшін TLS параметрлері

SMTP сервері осы протоколды қолдайтын болса, TLS қолдануды өшіре аласыз, TLS қолдана аласыз немесе тек TLS-ті күштеп қолдана аласыз. Егер сіз тек TLS пайдалануды ұйғарсаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, тек TLS пайдалануды ұйғарсаңыз, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификат көрсете аласыз.

- SMTP серверінің сертификаты файлын таңдаңыз

Сертификаттар тізімі бар файлды сенімді сертификаттау орталығынан (CA) ала аласыз және оны Kaspersky Security Center бағдарламасына жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт кодталмаған болса, құпиясөзде бос мән болуы мүмкін. **Хабарландыру хабары** өрісінде оқиға орын алған кезде қолданба жіберетін оқиға туралы ақпараты бар стандартты мәтін болады. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер бар. Хабар мәтінін, оқиғаның егжей-тегжейлі деректері бар жаңа алмастырылатын параметрлерді қосу арқылы өзгертуге болады. Алмастырылатын параметрлер тізімі өрістің оң жағындағы түймені басу арқылы қолжетімді.

Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Тексеру хабарын жіберу түймесі арқылы хабарландырулардың дұрыс конфигурацияланғанын тексеріңіз. Бағдарлама көрсетілген алушыларға мәтіндік хабарлар жібереді.

- **Іске қосылатын орындалатын файл**

  Егер бұл хабарландыру тәсілі таңдалса, енгізу өрісінде оқиға болған кезде қандай бағдарлама іске қосылатынын көрсетуге болады.

  Хабарландырулар санының шегін конфигурациялау сілтемесінен өту кезінде, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

  Сынақ хабарын жіберу түймесін басу арқылы, хабарлардың дұрыс конфигурацияланғанын тексеруге болады: бағдарлама көрсетілген электрондық пошта мекенжайларына мәтіндік хабарлар жібереді.

5. **Хабарландыру хабары** өрісінде оқиға болған кезде бағдарлама жіберетін мәтінді енгізіңіз.

   Мәтін өрісінің оң жағында орналасқан ашылмалы тізімнен хабарға оқиғаның егжей-тегжейі бар алмастырылатын параметрлерді қосуға болады (мысалы, оқиғаның сипаттамасы, пайда болу уақыты және т.б.).

   Хабарландыру мәтінінде % белгішесі болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

6. **Тексеру хабарын жіберу** түймесі арқылы хабарландырулардың дұрыс конфигурацияланғанын тексеріңіз.

   Бағдарлама көрсетілген алушыға сынақ хабарын жібереді.

7. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

Нәтижесінде, конфигурацияланған хабарландыру параметрлері клиент құрылғыларында болып жатқан барлық оқиғаларға таралады.

Оқиғаларды конфигурациялау бөлімінде, Басқару сервері параметрлерінде, саясат параметрлерінде немесе бағдарлама параметрлерінде белгіленген оқиғалар үшін хабарландыру параметрлерінің мәндерін өзгертуге болады.

Хабарландыруларды таратуды тексеру

Оқиға туралы хабарландырулардың таралуын тексеру үшін клиент құрылғыларында Eicar сынақ "вирусын" анықтау туралы хабарландыру қолданылады.

Оқиғалар туралы хабарландырулардың таралуын тексеру үшін:

1. Клиент құрылғысындағы файлдық жүйені нақты уақыт режимінде қорғау тапсырмасын тоқтатыңыз және Eicar сынақ "вирусын" клиент құрылғысына көшіріңіз. Файлдық жүйені нақты уақыт режимінде қорғау тапсырмасын қайта қосыңыз.

2. Басқару тобына немесе Eicar "вирусы" бар клиент құрылғысын қамтитын құрылғылар жиынтығына арналған клиент құрылғыларын тексеру тапсырмасын іске қосыңыз.

   Егер сканерлеу тапсырмасы дұрыс конфигурацияланған болса, оны орындау барысында сынақ "вирусы" анықталады. Егер хабарландыру параметрлері дұрыс конфигурацияланған болса, сіз табылған вирус туралы хабарландыру аласыз.

Басқару сервері түйінінің жұмыс аймағында, **Оқиғалар** қойыншасында, **Соңғы оқиғалар** таңдауында "вирустың" анықталғаны туралы жазба көрсетіледі.

Eicar сынақ "вирусында" сіздің құрылғыңызға зиян тигізуі мүмкін бағдарламалық код жоқ. Алайда өндірушілердің қауіпсіздік қолданбаларының көпшілігі бұл файлды вирус деп анықтайды. Сынақ "вирусын" EICAR ұйымының ресми сайтынан жүктеп алуға болады.

Орындалатын файл көмегімен оқиғалар туралы хабарлау

Kaspersky Security Center орындалатын файлды іске қосу арқылы әкімшіге клиент құрылғыларындағы оқиғалар туралы хабарлауға мүмкіндік береді. Орындалатын файлда әкімшіге жіберілетін оқиғаның алмастырылатын параметрлері бар басқа орындалатын файл болуы керек (төмендегі кестені қараңыз).

Оқиғаны сипаттауға арналған алмастырылатын параметрлер

Алмастырылатын параметр	Алмастырылатын параметр сипаттамасы
%SEVERITY%	Оқиғаның маңыздылық деңгейі. Ықтимал мәндер: • **Ақпараттық** • **Ескерту** • **Сәтсіз аяқталды** • **Критикалық**
%COMPUTER%	Оқиға болған құрылғының атауы. Құрылғы атауының максималды ұзындығы - 256 таңба.
%DOMAIN%	Оқиға болған құрылғының домен атауы.
%EVENT%	Оқиға түрінің атауы. Оқиға түрінің атауының максималды ұзындығы - 50 таңба.
%DESCR%	Оқиғаның сипаттамасы. Максималды сипаттама ұзындығы - 1000 таңба.
%RISE_TIME%	Оқиғаны құру уақыты.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Тапсырманың атауы. Тапсырма атауының максималды ұзындығы - 100 таңба.
%KL_PRODUCT%	Бағдарлама атауы.
%KL_VERSION%	Қолданба нұсқасының нөмірі.
%KLCSAK_EVENT_SEVERITY_NUM%	Оқиғаның маңыздылық деңгейінің коды. Ықтимал мәндер: • 1 – **Ақпараттық**. • 2 – **Ескерту**. • 3 – **Сәтсіздік**. • 4 – **Критикалық**.
%HOST_IP%	Оқиға болған құрылғының IP мекенжайы.
%HOST_CONN_IP%	Оқиға болған құрылғы қосылымының IP мекенжайы.

Мысалы:
Оқиға туралы хабарлау үшін орындалатын файл қолданылады (мысалы, script1.bat), оның ішінде %COMPUTER% алмастырылатын параметрі бар басқа орындалатын файл іске қосылады (мысалы, script2.bat). Оқиға болған кезде әкімші құрылғысында script1.bat файлы іске қосылып, өз кезегінде %COMPUTER% параметрі бар script2.bat файлын іске қосады. Нәтижесінде, әкімші оқиға болған құрылғының атын алады.

TLS қосылымын шифрлау

Ұйымыңыздың желісіндегі осалдықтарды түзету үшін TLS протоколымен трафикті шифрлауды қосуға болады. Басқару серверде және iOS MDM серверінде TLS шифрлау протоколдарын және қолдау көрсетілетін шифрлау жиынтықтарын қосуға болады. Kaspersky Security Center жүйесі TLS протоколының 1.0, 1.1, 1.2 және 1.3 нұсқаларына қолдау көрсетеді. Сіз қажетті шифрлау протоколы мен шифрлау жиынтықтарын таңдай аласыз.

Kaspersky Security Center бағдарламасы өздігінен қол қойылатын сертификаттарды қолданады. iOS құрылғылары үшін қосымша конфигурациялау талап етілмейді. Сондай-ақ, сіз өзіңіздің сертификаттарыңызды да қолдана аласыз. Сенімді сертификаттау орталығы қол қойған сертификаттарды қолдану ұсынылады.

Басқару сервері

Басқару серверінде рұқсат етілген шифрлау протоколдары мен шифрлау жиынтықтарын конфигурациялау үшін:

1. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Әкімшілік серверде рұқсат етілген шифрлау протоколдары мен шифрлау жиынтықтарын орнату үшін SrvUseStrictSslSettings жалаушасын қолданыңыз. Келесі пәрменді енгізіңіз:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <мән> -t d
   ```

   SrvUseStrictSslSettings жалаушасының <мән> параметрін көрсетіңіз:

   - 4 – TLS протоколдарының тек 1.2 және 1.3 нұсқалары қосылған. Сондай-ақ TLS_RSA_WITH_AES_256_GCM_SHA384 бар шифрлау жиынтығы қосылған (бұл шифрлау жиынтықтары Kaspersky Security Center алдыңғы нұсқаларымен кері үйлесімділік үшін қажет). Бұл әдепкі бойынша мәні.

     TLS 1.2 протоколы қолдау көрсететін шифрлау жиынтықтары:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (TLS_RSA_WITH_AES_256_GCM_SHA384 шифр жинағымен)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     TLS 1.3 протоколы қолдау көрсететін шифрлау жиынтықтары:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256

- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

- 5 – TLS протоколдарының тек 1.2 және 1.3 нұсқалары қосылған. TLS протоколының 1.2 және 1.3 нұсқалары төменде берілген арнайы шифрлау жиынтықтарына қолдау көрсетеді.

  TLS 1.2 протоколы қолдау көрсететін шифрлау жиынтықтары:

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  TLS 1.3 протоколы қолдау көрсететін шифрлау жиынтықтары:

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

SrvUseStrictSslSettings жалауша параметрінің мәндері үшін 0, 1, 2 немесе 3 мәндерін пайдалану ұсынылмайды. Бұл параметр мәндері TLS протоколының қауіпті нұсқаларына (TLS 1.0 және TLS 1.1 протоколдары) және қауіпті шифрлау жиынтықтарына сәйкес келеді және Kaspersky Security Center бағдарламасының бұрынғы нұсқаларымен кері үйлесімділік үшін ғана пайдаланылады.

3. Kaspersky Security Center 15.1 келесі қызметтерін қайта іске қосыңыз:

   - Басқару сервері
   - Веб-сервер
   - Прокси-серверді белсендіру қызметі

TLS протоколы арқылы трафикті шифрлау қосылады.

KLTR_TLS12_ENABLED және KLTR_TLS13_ENABLED жалаушаларын сәйкесінше TLS 1.2 және 1.3 протоколдарына қолдау көрсетуді қосу үшін пайдалануға болады. Бұл жалаушалар әдепкі бойынша қосылады.

TLS 1.2 және 1.3 протоколдарына қолдау көрсетуді қосу немесе өшіру үшін:

1. klscflag утилитасын іске қосыңыз.

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Windows пәрмен жолында келесі пәрмендердің бірін әкімші құқықтарымен енгізіңіз:

   - TLS 1.2 протоколының қолдауын қосу немесе өшіру үшін осы пәрменді пайдаланыңыз:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <мән> -t d
     ```

   - TLS 1.3 протоколының қолдауын қосу немесе өшіру үшін осы пәрменді пайдаланыңыз:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <мән> -t d
     ```

   Жалаушаның < мән > параметрін көрсетіңіз:

   - `1` – TLS протоколының қолдауын қосу үшін.
   - `0` – TLS протоколының қолдауын өшіру үшін.

iOS MDM сервері

iOS құрылғылары мен iOS MDM сервері арасындағы қосылым шифрланған.

iOS MDM серверінде рұқсат етілген шифрлау протоколдары мен шифрлау жиынтықтарын конфигурациялау үшін:

1. iOS MDM сервері орнатылған клиент құрылғысының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.
2. Келесі бөлімге өтіңіз:

   - 32 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor

   - 64 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI

3. `StrictSslSettings` атты кілт жасаңыз.
4. Кілт түрін `DWORD` деп көрсетіңіз.
5. Кілт мәнін белгілеңіз:

   - `2` – TLS 1.0, TLS 1.1 және TLS 1.2 протоколдары қосылған.
   - `3` – тек TLS 1.2 протоколы қосылған (әдепкі мән).

6. Kaspersky Security Center бағдарламасының iOS MDM серверінің қызметін қайта іске қосыңыз.

Интерфейсті конфигурациялау

Kaspersky Security Center интерфейсін конфигурациялай аласыз:

- Пайдаланылатын функцияларға байланысты консоль ағашында, жұмыс аймағында және нысан сипаттарының терезелерінде (қалталар, бөлімдер) нысандарды көрсету және жасыру.
- Басты терезе элементтерін көрсету және жасыру (мысалы, консоль ағашы немесе **Әрекеттер** мен **Көру** сияқты стандартты мәзірлер).

Kaspersky Security Center интерфейсін қазіргі уақытта қолданылатын функциялар жиынтығына сәйкес конфигурациялау үшін, келесі әрекеттерді таңдаңыз:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Бағдарламаның басты терезесі мәзірінде **Көру** → **Интерфейсті конфигурациялау** тармағын таңдаңыз.
3. Ашылған **Интерфейсті конфигурациялау** терезесінде келесі жалаушаларды пайдаланып, интерфейс элементтерін көрсетуді конфигурациялаңыз:

   - **Осалдықтар мен патчтарды басқаруды көрсету**

     Бұл параметр қосулы болса, **Қашықтан орнату** қалтасында **Құрылғылар үлгілерін жаю** ішкі қалтасы көрсетіледі, ал **Қоймалар** қалтасында **Жабдық** ішкі қалтасы көрсетіледі.

     Бағдарламаны жылдам іске қосу шебері аяқталмаса, бұл параметр әдепкі бойынша өшіріледі. Бағдарламаны жылдам іске қосу шебері аяқталған болса, бұл параметр әдепкі бойынша қосылған.

     > Бұл параметр өшірулі болса, Желілік басқару мүмкіндіктеріне жарамды лицензияңыз болса да, **RDP сессиясын жасау** және **Windows компьютерлік бөлісу қызметін пайдалану** мәзір тармақтары қолжетімді болмайды.

   - **Деректерді шифрлауды және қорғауды көрсету**

     Бұл параметр қосулы болса, консоль ағашында **Деректерді шифрлау және қорғау** қалтасы көрсетіледі.

     Әдепкі бойынша, параметр қосулы.

   - **Соңғы нүктелерді басқару параметрлерін көрсету**

     Бұл параметр қосулы болса, Kaspersky Endpoint Security for Windows сипаттар терезесінің **Қауіпсіздікті бақылау** бөлімінде келесі бөлікшелер көрсетіледі:

     - **Бағдарламаны басқару**
     - **Құрылғыны басқару**
     - **Веб-бақылау**
     - **Аномалияларды бейімделумен басқару**

     Осы параметр өшірулі болса, бұл бөлікшелер **Қауіпсіздікті бақылау** бөлімінде көрсетіледі.

     Әдепкі бойынша, параметр қосулы.

- **Ұялы құрылғыларды басқару тармағын көрсету**

  Бұл параметр қосулы болса, **Ұялы құрылғыларды басқару** мүмкіндіктері қолжетімді. Бағдарламаны іске қосқаннан кейін, консоль ағашында **Ұялы құрылғылар** қалтасы көрсетіледі.

  Әдепкі бойынша, параметр қосулы.

- **Қосалқы Басқару серверлерін көрсету**

  Егер жалауша қойылса, консоль ағашында басқару топтарындағы қосалқы және виртуалды Басқару серверлерінің түйіндері көрсетіледі. Бұл ретте, қосалқы және виртуалды Басқару серверлерімен байланысты функциялар қолжетімді, мысалы, бағдарламаларды қосалқы Басқару серверлеріне қашықтан орнату үшін тапсырмалар жасау.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Қауіпсіздік параметрлері бар тарауларды көрсету**

  Егер бұл параметр қосулы болса, **Қауіпсіздік** бөлімі Басқару сервері сипаттары, басқару топтары және басқа нысандар терезесінде көрсетіледі. Бұл параметр пайдаланушылар мен пайдаланушылар топтарына нысандармен жұмыс істеу үшін конфигурацияланатын құқықтарды беруге мүмкіндік береді.

  Әдепкі бойынша, параметр өшірулі.

4. **OK** түймесін басыңыз.

Кейбір өзгертулерді қолдану үшін бағдарламаның басты терезесін жауып, оны қайтадан ашу керек.

Бағдарламаның негізгі терезесінде элементтердің көрсетілуін конфигурациялау үшін:

1. Бағдарламаның басты терезесінің мәзірінде **Көру** → **Конфигурациялау** тармағын таңдаңыз.
2. Ашылған **Көруді конфигурациялау** терезесінде басты терезенің элементтерін жалаушалардың көмегімен көрсетуді конфигурациялаңыз.
3. **OK** түймесін басыңыз.

Желідегі құрылғыларды табу

Бұл бөлімде Kaspersky Security Center орнатқаннан кейін орындау керек қадамдар сипатталған.

Сценарий: Желілік құрылғыларды табу

Қауіпсіздік бағдарламаларын орнатпас бұрын құрылғыларды іздеу керек. Басқару сервері анықталған құрылғылар туралы ақпаратты алады және саясаттардың көмегімен құрылғыларды басқаруға мүмкіндік береді. Желіде қолжетімді құрылғылар тізімін жаңарту үшін тұрақты желі сауалнамалары қажет.

Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

Желілік құрылғыларды анықтау келесі кезеңдерді қамтиды:

1. **Құрылғыларды табу**

   Бағдарламаны жылдам іске қосу шебері құрылғыларды бастапқы табуды орындайды және компьютерлер, планшеттер және ұялы телефондар сияқты желілік құрылғыларды табуға көмектеседі. Сіз құрылғыларды табуды қолмен де іске қоса аласыз.

2. **Сауалнамалар кестесін конфигурациялау**

   Сауалнаманың қандай түрін үнемі қолданғыңыз келетінін анықтаңыз. Қажетті түрлерді қосыңыз және сауалнама кестесін конфигурациялаңыз. Сондай-ақ, желіде сауалнама өткізу жиілігі бойынша ұсыныстарды қараңыз.

3. **Табылған құрылғыларды басқару топтарына қосу ережелерін орнату (қажет болса)**

   Желіде жаңа құрылғылар пайда болса, олар әдеттегі сауалнамалар кезінде табылып, **Тағайындалмаған құрылғылар** тобына автоматты түрде қосылады. Құрылғыларды **Басқарылатын құрылғылар** тобына таратылатын құрылғыны жылжыту ережелерін конфигурациялауға болады. Сондай-ақ, сақтау ережелерін конфигурациялауға болады.

   3-қадамды өткізіп жіберсеңіз, жаңадан табылған құрылғылар тізімі **Тағайындалмаған құрылғылар** тобында орналасқан. Сіз осы құрылғыларды **Басқарылатын құрылғылар** тобына қолмен жылжыта аласыз. Құрылғыларды **Басқарылатын құрылғылар** тобына қолмен жылжытқан болсаңыз, онда сіз құрылғылардың әрқайсысы туралы ақпаратты талдап, оны басқару тобына және қайсысына жылжыту керектігін шеше аласыз.

Нәтижелер

Сценарийдің аяқталуы арқасында:

- Kaspersky Security Center Басқару сервері желідегі құрылғыларды анықтайды және олар туралы ақпарат береді.
- Желінің болашақ сауалнамалары және оларды іске қосу кестесі конфигурацияланды.
- Жаңадан табылған құрылғылар конфигурацияланған ережелерге сәйкес орналастырылады. (Болмаса ережелер конфигурацияланбаса, құрылғылар **Тағайындалмаған құрылғылар** тобында қалады).

Тағайындалмаған құрылғылар

Бұл бөлімде басқару топтарына кірмейтін ұйым желісінің құрылғыларымен жұмыс істеу туралы ақпарат берілген.

Құрылғыларды табу

Бұл бөлімде Kaspersky Security Center бағдарламасында қолжетімді құрылғыларды анықтау түрлері сипатталған, сонымен қатар олардың әрқайсысын пайдалану туралы ақпарат берілген.

Тұрақты желілік сауалнамалар кезінде Басқару сервері желінің құрылымы мен желідегі құрылғылар туралы ақпарат алады. Деректер Басқару сервері дерекқорына жазылады. Басқару сервері желі сауалнамаларының келесі түрлерін жүргізе алады:

- **Windows желісінің сауалнамасы**. Басқару сервері Windows желісінің сауалнамасының екі түрін жүргізе алады: жылдам және толық. Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады. Толық сауалнама әрбір клиент құрылғысынан операциялық жүйенің атауы, IP мекенжайы, DNS атауы және NetBIOS атауы сияқты қосымша мәліметтерді сұрайды. Жылдам және толық сауалнама әдепкі бойынша қосылған. Windows желісінің сауалнамасы кезінде құрылғыларды анықтау мүмкін болмауы ықтимал, мысалы, роутер немесе желі экраны UDP 137, UDP 138, TCP 139 порттарын жауып тастаса.

- **Active Directory сауалнамасы**. Басқару сервері Active Directory топтарының құрылымы туралы ақпаратты, сондай-ақ Active Directory топтарына кіретін құрылғылардың DNS атаулары туралы ақпаратты алады. Сауалнаманың бұл түрі әдепкі бойынша қосылған. Active Directory пайдаланбасаңыз, Active Directory сауалнамасын пайдалануға кеңес береміз, әйтпесе басқару сервері ешқандай құрылғыны таппайды. Active Directory қолданбасаңыз, бірақ бөлек желілік құрылғылар оның мүшелері болмаса, бұл құрылғыларды Active Directory сауалнамасы барысында анықтау мүмкін болмайды.

- **IP ауқымдарының сауалнамасы**. Басқару сервері ICMP пакеттері немесе NBNS протоколдары арқылы көрсетілген IP ауқымдарына сауалнама жүргізеді және IP ауқымдарына кіретін құрылғылар туралы толық ақпарат алады. Сауалнаманың бұл түрі әдепкі бойынша өшірілген. Егер сіз Windows желісінің сауалнамасын және/немесе Active Directory сауалнамасын қолданбасаңыз, сауалнаманың бұл түрін пайдалану ұсынылмайды.

- **Zeroconf сауалнамасы**. Тарату нүктесі нөлдік конфигурациясы бар желіні қолдана отырып, IPv6 желісіне сауалнама өткізеді (бұдан әрі *Zeroconf* деп те аталады). Сауалнаманың бұл түрі әдепкі бойынша өшірілген. Тарату нүктесі Linux жүйесінде жұмыс істеп тұрса, Zeroconf сауалнамасын пайдалануға болады.

Егер сіз құрылғыларды жылжыту ережелерін конфигурациялап, қосқан болсаңыз, табылған жаңа құрылғылар автоматты түрде **Басқарылатын құрылғылар** тобына ауысады. Егер құрылғыларды жылжыту ережелері қосылмаған болса, табылған жаңа құрылғылар автоматты түрде **Тағайындалмаған құрылғылар** тобына ауысады.

Әр түрге арналған құрылғыны анықтау параметрлерін өзгертуге болады. Мысалы, сауалнама кестесін өзгерту немесе бүкіл домендер тобына немесе тек белгілі бір доменге сауалнама жүргізу қажет екенін көрсету керек болуы мүмкін.

Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

Windows желісінің сауалнамасы

Windows желісінің сауалнамасы туралы

Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады. Толық сауалнама барысында, әрбір клиент құрылғысынан келесі ақпарат сұралады:

- Операциялық жүйенің аты

- IP мекенжайы

- DNS атауы
- NetBIOS атауы

Жылдам сауалнама кезінде де, толық сауалнама кезінде де керегі:

- UDP 137/138, TCP 139, UDP 445, TCP 445 ашық порттары.
- Қосулы SMB протоколы.
- Microsoft Computer Browser қызметі қолданылуы тиіс, ал негізгі браузер рөлін атқаратын құрылғы Басқару серверінде қолжетімді болуы керек;
- Microsoft Computer Browser қызметі қолданылуы тиіс, ал негізгі браузер рөлін атқаратын құрылғы клиент құрылғысында қолжетімді болуы керек:
  - Желілік құрылғылардың саны 32-ден аспаса, кемінде бір құрылғының болуы.
  - Әрбір 32 желілік құрылғыға кемінде бір құрылғының болуы.

Желінің толық сауалнамасы, егер жылдам сауалнама кемінде бір рет іске қосылған болса ғана іске қосылуы тиіс.

Windows желісінің сауалнамасы параметрлерін көру және өзгерту

Windows желісінің сауалнамасы параметрлерін өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **Домендер** салынған қалтасын таңдаңыз.

   Қазір сауалнама өткізу түймесін басу арқылы **Тағайындалмаған құрылғылар** қалтасынан **Құрылғыны табу** қалтасына өтуге болады.

   Домендер ішкі қалтасының жұмыс аймағында құрылғылар тізімі көрсетіледі.

2. **Қазір сауалнама өткізу** түймесін басыңыз.

   Домен сипаттары терезесі ашылады. Қажет болса, Windows желісінің сауалнамасы параметрлерін конфигурациялаңыз:

   - **Windows желілік сауалнамасын қосу**

     Әдепкі бойынша, осы нұсқа таңдалады. Егер сізге Windows желісінің сауалнамасын жүргізу қажет болмаса (мысалы, Active Directory сауалнамасы жеткілікті болса), сіз бұл параметрді алып тастай аласыз.

   - **Жылдам сауалнама жүргізу кестесін орнату**

     Әдепкі бойынша уақыт аралығы 15 минутты құрайды.

     Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады.

     Әрбір кейінгі сауалнама кезінде алынған деректер алдыңғы деректерді толығымен алмастырады.

     Желіде сауалнама өткізу кестесінің келесі нұсқалары қолжетімді:

     - **N күн сайын**

       Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

- **N минут сайын**

  Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

  Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

- **Апта күндері бойынша**

  Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр қосулы.

- **Толық сауалнама жүргізу кестесін орнату**

  Әдепкі бойынша, сауалнама кезеңі бір сағатты құрайды. Әрбір кейінгі сауалнама кезінде алынған деректер алдыңғы деректерді толығымен алмастырады.

  Желіде сауалнама өткізу кестесінің келесі нұсқалары қолжетімді:

  - **N күн сайын**

    Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

    Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

  - **N минут сайын**

    Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

    Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

  - **Апта күндері бойынша**

    Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

    Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

  - **Ай сайын, таңдалған апталардың көрсетілген күндері**

    Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

    Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр қосулы.

Желіде сауалнама өткізуді бірден іске қосу қажет болса, **Қазір сауалнама өткізу** түймесін басыңыз. Сауалнаманың екі түрі де іске қосылады.

Виртуалды Басқару серверінде Windows желісінің сауалнамасы параметрлерін қарау және өзгерту әрекеттері тарату нүктесінің сипаттары терезесінде, **Құрылғыны табу** бөлімінде жүзеге асырылады.

Active Directory сауалнамасы

Active Directory қолдансаңыз, Active Directory сауалнамасын қолданыңыз; не болмаса, сауалнамалардың басқа түрлерін қолдану ұсынылады. Active Directory қолдансаңыз, бірақ бөлек желілік құрылғылар оның мүшелері болмаса, бұл құрылғыларды Active Directory сауалнамасы барысында анықтау мүмкін болмайды.

Active Directory сауалнама нәтижелері келесі сауалнама нәтижелеріне қарамастан басқару серверінде 30 күн бойы сақталады.

Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

Active Directory сауалнамасының параметрлерін көру және өзгерту

Active Directory топтары сауалнамасының параметрлерін көру және өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **Active Directory** салынған қалтасын таңдаңыз.

   Болмаса **Қазір сауалнама өткізу** түймесін басу арқылы **Тағайындалмаған құрылғылар** қалтасынан **Құрылғыны табу** қалтасына ауысуға болады.

2. **Сауалнама параметрлерін конфигурациялау** түймесін басыңыз.

   Нәтижесінде, Active Directory сипаттары терезесі ашылады. Қажет болса, Active Directory топтары сауалнамасының параметрлерін конфигурациялаңыз:

   - **Active Directory сауалнамасын қосу**

     Әдепкі бойынша, осы нұсқа таңдалады. Алайда, Active Directory қолданылмаса, сауалнама нәтижелерінде ештеңе табылмайды. Бұл жағдайда, сіз осы параметрді таңдаудан бас тарта аласыз.

   - **Сауалнама кестесін орнату**

     Әдепкі бойынша, сауалнама кезеңі бір сағатты құрайды.

     Желіде сауалнама өткізу кестесінің келесі нұсқалары қолжетімді:

     - **N күн сайын**

Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

- **N минут сайын**

  Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

  Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

- **Апта күндері бойынша**

  Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр қосулы.

- **Кеңейтілген**

  Сауалнама үшін Active Directory домендерін таңдауға болады:

  - Kaspersky Security Center қатысты болып келетін Active Directory домені.
  - Kaspersky Security Center қатысты болып келетін домендер тобы.
  - Active Directory көрсетілген домендер тізімі.

    Бұл параметрді таңдаған кезде сауалнама аймағына домендерді қосуға болады:

    - **Қосу** түймесін басыңыз.
    - Тиісті өрістерде домендік контроллердің мекенжайын, сондай-ақ оған кіру үшін есептік жазбаның атауы мен құпиясөзін көрсетіңіз.
    - Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

    Тізімнен домендік контроллер мекенжайын таңдап, оны өзгерту немесе жою үшін **Өзгерту** немесе **Жою** түймесін басуға болады.

  - Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

Желіде сауалнама өткізуді бірден іске қосу қажет болса, **Қазір сауалнама өткізу** түймесін басыңыз.

Виртуалды Басқару серверінде Active Directory топтары сауалнамасы параметрлерін қарау және өзгерту әрекеттері тарату нүктесінің сипаттары терезесінде, **Құрылғыны табу** бөлімінде жүзеге асырылады.

IP ауқымдарының сауалнамасы

Басқару сервері ICMP пакеттері немесе NBNS протоколдары арқылы көрсетілген IP ауқымдарына сауалнама жүргізеді және IP ауқымдарына кіретін құрылғылар туралы толық ақпарат алады. Сауалнаманың бұл түрі әдепкі бойынша өшірілген.

Microsoft Active Directory немесе Samba домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` мен `workgroup` параметрлерін көрсетіңіз. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту

IP ауқымы топтарының сауалнамасы параметрлерін көру және өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **IP ауқымдары** салынған қалтасын таңдаңыз.

   Сіз **Қазір сауалнама өткізу** түймесі арқылы **Құрылғыны табу** қалтасынан **Тағайындалмаған құрылғылар** қалтасына ауыса аласыз.

2. Қаласаңыз, сауалнама үшін IP ауқымын қосу үшін **IP ауқымдары** ішкі қалтасында **Қосалқы желіні қосу** түймесін, содан соң **OK** түймесін басыңыз.

3. **Сауалнама параметрлерін конфигурациялау** түймесін басыңыз.

   IP ауқымдары сипаттары терезесі ашылады. Қажет болса, IP ауқымдарының сауалнамасы параметрлерін ауыстыруға болады:

   - **IP ауқымы бойынша сауалнама өткізуді қосу**

     Әдепкі бойынша, бұл нұсқа таңдалмаған. Егер сіз Windows желісінің сауалнамасын және/немесе Active Directory сауалнамасын қолдансаңыз, сауалнаманың бұл түрін пайдалану ұсынылмайды.

   - **Сауалнама кестесін орнату**

     Әдепкі бойынша уақыт аралығы 420 минутты құрайды. Әрбір кейінгі сауалнама кезінде алынған деректер алдыңғы деректерді толығымен алмастырады.

     Желіде сауалнама өткізу кестесінің келесі нұсқалары қолжетімді:

     - **N күн сайын**

       Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

       Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

- **N минут сайын**

  Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

  Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

- **Апта күндері бойынша**

  Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр қосулы.

Желіде сауалнама өткізуді бірден іске қосу қажет болса, **Қазір сауалнама өткізу** түймесін басыңыз. Бұл түйме, тек **IP ауқымы бойынша сауалнама өткізуді қосу** параметрі таңдалса ғана қолжетімді болады.

Виртуалды Басқару серверінде IP ауқымдарының сауалнамасы параметрлерін қарау және өзгерту әрекеттері тарату нүктесінің сипаттары терезесінде, **Құрылғыны табу** бөлімінде жүзеге асырылады. IP ауқымдарының сауалнамасы нәтижесінде табылған клиент құрылғылары виртуалды Сервердің **Домендер** қалтасында көрсетіледі.

Zeroconf сауалнамасы

Сауалнаманың бұл түріне тек Linux операциялық жүйелері бар тарату нүктелері үшін қолдау көрсетіледі.

Тарату нүктесі IPv6 мекенжайы бар құрылғыларға ие желілерді сұрастыра алады. Бұл жағдайда, IP ауқымдары көрсетілмейді, ал тарату нүктесі нөлдік конфигурациясы бар желіні (бұдан әрі *Zeroconf* деп те аталады) қолдану арқылы бүкіл желіде сауалнама жүргізеді. Zeroconf пайдалануды бастау үшін тарату нүктесінде avahi-browse утилитасын орнату керек.

Zeroconf сауалнамасын қосу үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **IP ауқымдары** салынған қалтасын таңдаңыз.

   Сіз **Қазір сауалнама өткізу** түймесі арқылы **Құрылғыны табу** қалтасынан **Тағайындалмаған құрылғылар** қалтасына ауыса аласыз.

2. **Сауалнама параметрлерін конфигурациялау** түймесін басыңыз.

3. IP ауқымдары сипаттарының ашылған терезесінде **Zeroconf технологиясымен сауалнаманы қосу** тармағын таңдаңыз.

Осыдан кейін, тарату нүктесі сіздің желіңізге сауалнама жүргізе бастайды. Бұл жағдайда, көрсетілген IP ауқымдары еленбейді.

Windows домендерімен жұмыс істеу. Домен параметрлерін көру және өзгерту

Домен параметрлерін өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **Домендер** салынған қалтасын таңдаңыз.

2. Доменді таңдап, оның сипаттары терезесін келесі тәсілдерінің бірімен ашыңыз:

   - Доменнің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   - **Топ сипаттарын көрсету** сілтемесі бойынша.

Сипаттар: <Домен атауы> терезесі ашылған соң, таңдалған домен параметрлерін конфигурациялауға болады.

Тағайындалмаған құрылғылар үшін сақтау ережелерін конфигурациялау

Windows желісінде сауалнамалар аяқталғаннан кейін, анықталған құрылғылар Тағайындалмаған құрылғылар басқару тобының ішкі топтарына орналастырылады. Бұл басқару тобы келесі жол бойынша орналасқан: **Қосымша** → **Құрылғыны табу** → **Домендер**. **Домендер** қалтасы тектік топ болып саналады. Қалтада, желіде сауалнама өткізу барысында анықталған домендер мен жұмыс топтарына сай келетін аттары бар еншілес топтар кіреді. Тектік топта ұялы құрылғыларды басқару топтары да болуы мүмкін. Сіз тектік басқару тобы үшін және әрбір еншілес топ үшін тағайындалмаған құрылғыларды сақтау ережелерін конфигурациялай аласыз. Сақтау ережелері желіде сауалнама өткізу параметрлеріне тәуелді емес және желі сауалнамасы өшірулі болса да жұмыс істей береді.

Тағайындалмаған құрылғыларды сақтау ережелерін конфигурациялау үшін:

1. **Құрылғыны табу** қалтасындағы консоль ағашында келесі әрекеттердің бірін орындаңыз:

   - Тектік топтың параметрлерін конфигурациялау үшін **Домендер** қалтасының контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

     Тектік топ сипаттары терезесі ашылады.

   - Еншілес топ параметрлерін конфигурациялау үшін, еншілес топтың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

     Еншілес топ сипаттары терезесі ашылады.

2. **Құрылғылар** бөлімінде келесі параметрлерді көрсетіңіз:

   - **Мына уақыттан көбірек белсенді емес болса, құрылғыны топтан жойыңыз (тәулік)**

     Егер бұл параметр қосулы болса, құрылғы басқару тобынан автоматты түрде жойылатын уақыт аралығын көрсетуге болады. Әдепкі бойынша бұл параметр еншілес топтарға таралады. Әдепкі бойынша белгіленген уақыт аралығы – 7 күн.

     Әдепкі бойынша, параметр қосулы.

   - **Тектік топтан иелену**

     Бұл параметр өшірулі болса, ағымдағы топтағы құрылғылар үшін сақтау кезеңі тектік топтан иеленеді және өзгертіле алмайды.

     Бұл параметр тек еншілес топтар үшін ғана қолжетімді.

     Әдепкі бойынша, параметр қосулы.

   - **Еншілес топтарда мәжбүрлеп иелену**

     Параметрлер мәндері еншілес топтарға бөлінеді, бірақ еншілес топтардың сипаттарында бұл параметрлер өзгертулер үшін қолжетімді емес.

     Әдепкі бойынша, параметр өшірулі.

Сіздің өзгертулеріңіз сақталды және қолданылды.

IP ауқымдарымен жұмыс істеу

Сіз қолданыстағы IP ауқымдарының параметрлерін конфигурациялай аласыз, сонымен қатар жаңа IP ауқымдарын жасай аласыз.

IP ауқымын жасау

IP ауқымын жасау үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **IP ауқымдары** салынған қалтасын таңдаңыз.
2. Қалтаның контекстік мәзірінен **Жаңа** → **IP ауқымы** тармағын таңдаңыз.
3. Ашылған **Жаңа IP ауқымы** терезесінде жасалып жатқан IP ауқымы параметрлерін конфигурациялаңыз.

Нәтижесінде, жасалған IP ауқымы **IP ауқымдары** қалтасының құрамында пайда болады.

IP ауқымдары параметрлерін көру және өзгерту

IP ауқымдары параметрлерін өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **IP ауқымдары** салынған қалтасын таңдаңыз.
2. IP ауқымын таңдап, оның сипаттары терезесін келесі тәсілдерінің бірімен ашыңыз:
   - IP ауқымының контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.
   - **Топ сипаттарын көрсету** сілтемесі бойынша.

Сипаттар: <IP ауқымы атауы> терезесі ашылған соң, таңдалған IP ауқымы параметрлерін конфигурациялауға болады.

Active Directory топтарымен жұмыс істеу Топ параметрлерін қарап шығу және өзгерту

Active Directory тобының параметрлерін өзгерту үшін:

1. **Құрылғыны табу** қалтасындағы консоль шежіресінен **Active Directory** салынған қалтасын таңдаңыз.
2. Active Directory тобын таңдап, оның сипаттары терезесін келесі тәсілдердің бірімен ашыңыз:
   - IP ауқымының контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.
   - **Топ сипаттарын көрсету** сілтемесі бойынша.

Сипаттар: <Active Directory тобының атауы> терезесі ашылған соң, онда таңдалған Active Directory тобының параметрлерін конфигурациялауға болады.

Құрылғыларды басқару топтарына автоматты түрде жылжыту ережелерін құру

Ұйым желісіне сауалнама жүргізу кезінде анықталатын құрылғыларды басқару топтарына автоматты түрде жылжытуды конфигурациялауға болады.

Құрылғыларды басқару топтарына автоматты түрде жылжыту ережелерін конфигурациялау үшін:

1. Консоль ағашында **Тағайындалмаған құрылғылар** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында **Ережелерді конфигурациялау** түймесін басыңыз.

Сипаттар: Тағайындалмаған құрылғылар терезесі ашылады. **Құрылғыларды жылжыту** бөлімінде құрылғыларды басқару топтарына автоматты түрде жылжыту ережелерін конфигурациялаңыз.

Құрылғы тізімдегі бірінші қолданылатын ережені орындайды (тізімде жоғарыдан төмен).

Клиент құрылғыларында VDI динамикалық режимін пайдалану

Ұйымның желісінде уақытша виртуалды машиналарды қолдана отырып, виртуалды инфрақұрылымды орналастыруға болады. Kaspersky Security Center бағдарламасы уақытша виртуалды машиналарды анықтайды және олар туралы деректерді Басқару сервері дерекқорына қосады. Пайдаланушы уақытша виртуалды машинамен жұмыс істеп болғаннан кейін, машина виртуалды инфрақұрылымнан алынып тасталады. Дегенмен, қашықтағы виртуалды машина туралы жазба Басқару серверінің дерекқорында сақталуы мүмкін. Сонымен қатар, жоқ виртуалды машиналар Басқару консолінде көрсетілуі мүмкін.

Жоқ виртуалды машиналар туралы деректердің сақталуын болдырмау үшін Kaspersky Security Center бағдарламасында Virtual Desktop Infrastructure (VDI) үшін динамикалық режимді қолдау іске асырылған. Әкімші VDI үшін динамикалық режимді қолдауды уақытша виртуалды машинада орнатылатын Желілік агенттің орнату пакетінің сипаттарында қоса алады.

Уақытша виртуалдық машинаны өшіру кезінде, Желілік агент Басқару серверіне өшіру туралы хабарлайды. Виртуалды машина сәтті өшірілген жағдайда, ол Басқару серверіне қосылған құрылғылар тізімінен алынып тасталады. Виртуалды машинаны өшіру дұрыс орындалмаса және Желілік агент Серверіне өшіру туралы хабарландыруды жібермесе, қайталайтын сценарий қолданылады. Бұл сценарийге сәйкес, виртуалды машина Сервермен синхрондаудың үш сәтсіз әрекетінен кейін Басқару серверіне қосылған құрылғылар тізімінен жойылады.

Желілік агенттің орнату пакетінің сипаттарында VDI динамикалық режимін қосу

VDI динамикалық режимін қосу үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
2. Желілік агенттің орнату пакетінің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Сипаттар: Kaspersky Security Center Желілік агенті терезесі ашылады.
3. **Сипаттар: Kaspersky Security Center Желілік агенті** терезесінде **Кеңейтілген** бөлімін таңдаңыз.
4. **Кеңейтілген** бөлімінде **VDI үшін динамикалық режимді қосу** параметрін таңдаңыз.

Желілік агент орнатылған құрылғы VDI бөлігі болады.

VDI құрамына кіретін құрылғыларды табу

VDI құрамына кіретін тағайындалмаған құрылғыларды табу үшін:

1. **Тағайындалмаған құрылғылар** қалтасының контекстік мәзірінен **Іздеу** опциясын таңдаңыз.

   Virtual Desktop Infrastructure бір бөлгі болып табылатын барлық құрылғы тізімін көру үшін **Басқару сервері** қалтасының контекстік мәзірінен **Іздеу** опциясын таңдаңыз.

2. **Іздеу** терезесінде **Виртуалды машиналар** қойындысында **Virtual Desktop Infrastructure бөлігі** параметрлер блогының бөлігінде **Иә** параметрін таңдаңыз.

3. **Қазір табу** түймесін басыңыз.

Virtual Desktop Infrastructure (VDI) бөлігі болып табылатын тағайындалмаған құрылғылар тізімі көрсетіледі.

VDI құрамына кіретін құрылғыларды басқару тобына жылжыту

VDI құрамына кіретін құрылғыларды басқару тобына жылжыту үшін:

1. **Тағайындалмаған құрылғылар** қалтасының жұмыс аймағында **Ережелерді конфигурациялау** түймесін басыңыз.

   Нәтижесінде, **Тағайындалмаған құрылғылар** қалтасы сипаттары терезесі ашылады.

2. **Тағайындалмаған құрылғылар** қалтасының сипаттары терезесінде, **Құрылғыларды жылжыту** бөлімінде **Қосу** түймесін басыңыз.

   Жаңа ереже терезесі ашылады.

3. **Жаңа ереже** терезесінде **Виртуалды машиналар** бөлімін таңдаңыз.

4. **Виртуалды машина болып табылады** ашылмалы тізімінен **Иә** тармағын таңдаңыз.

Құрылғыларды басқару тобына жылжыту ережесі жасалады.

Жабдықты түгендеу

Жабдықты түгендеу үшін қолданылатын жабдықтар тізімінде (**Қоймалар** → **Жабдық**), екі тәсілмен толтырылады: автоматты түрде және қолмен. Әрбір желі сауалнамасынан кейін барлық анықталған құрылғы тізімге автоматты түрде қосылады; дегенмен желіде сауалнама өткізгіңіз келмесе, құрылғыларды қолмен қосуға болады. Тізімге маршрутизаторлар, принтерлер немесе құрылғы жабдықтары сияқты басқа құрылғыларды қолмен қосуға болады.

Құрылғының сипаттарында құрылғылар туралы толық ақпаратты көруге және өңдеуге болады.

Жабдықтар тізімінде келесі құрылғы түрлері болуы мүмкін:

- компьютерлер;
- ұялы құрылғылар;
- желілік құрылғылар;
- виртуалды құрылғылар;
- компьютер компоненттері;
- компьютерлік периферия;
- қосылатын құрылғылар;

- VoIP телефондары;
- желілік қоймалар.

Әкімші анықталған құрылғыларға *Корпоративтік кластың аппараттық жасақтамасы* белгісін беруі мүмкін. Бұл белгіні құрылғының сипаттарында қолмен тағайындауға немесе оны автоматты түрде тағайындау критерийлерін белгілеуге болады. Бұл жағдайда, *Корпоративтік кластың аппараттық жасақтамасы* белгісі құрылғының түрі бойынша белгіленеді.

Kaspersky Security Center жабдықты шығынға жазуға мүмкіндік береді. Бұл үшін, құрылғының сипаттарында **Құрылғы шығынға жазылды** параметрін таңдау керек. Мұндай құрылғы жабдықтар тізімінде көрсетілмейді.

Әкімші **Жабдық** қалтасындағы бағдарламаланатын логикалық контроллерлер (БЛК) тізімімен жұмыс істей алады. БЛК тізімдерімен жұмыс істеу туралы толық ақпарат *Kaspersky Industrial Cyber Security for Nodes пайдаланушы нұсқаулығында* келтірілген.

Жаңа құрылғылар туралы ақпаратты қосу

Желідегі жаңа құрылғылар туралы ақпаратты қосу үшін:

1. **Қоймалар** қалтасындағы консоль шежіресінен **Жабдық** салынған қалтасын таңдаңыз.
2. **Жабдық** қалтасының жұмыс аймағында, **Құрылғыны қосу** түймесі арқылы **Жаңа құрылғы** терезесін ашыңыз.

   Жаңа құрылғы терезесі ашылады.
3. **Жаңа құрылғы** терезесінде, **Түрі** ашылмалы тізімінде қосқыңыз келетін құрылғы түрін таңдаңыз.
4. **ОК** түймесін басыңыз.

   Жалпы бөліміндегі құрылғы сипаттары терезесі ашылады.
5. **Жалпы** бөлімінде құрылғы туралы деректерді енгізу өрістерін толтырыңыз. **Жалпы** бөлімінде келесі параметрлер қолжетімді:
   - **Корпоративтік құрылғы**. Егер сіз құрылғыға *Корпоративтік* белгісін бергіңіз келсе, жалаушаны қойыңыз. Осы белгі бойынша құрылғыларды **Жабдық** қалтасынан іздеуге болады.
   - **Құрылғы шығынға жазылды**. Егер сіз құрылғының **Жабдық** қалтасындағы құрылғылар тізімінде пайда болуын қаламасаңыз, жалаушаны қойыңыз.
6. **Қолдану** түймесін басыңыз.

Жаңа құрылғы **Жабдық** қалтасының жұмыс аймағында көрсетіледі.

Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау

Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау үшін:

1. **Қоймалар** қалтасындағы консоль шежіресінен **Жабдық** салынған қалтасын таңдаңыз.
2. **Жабдық** қалтасының жұмыс аймағында **Қосымша әрекеттер** түймесін басып, ашылмалы тізімнен **Корпоративтік құрылғылар үшін ережені орнату** тармағын таңдаңыз.

   Жабдық сипаттары терезесі ашылады.
3. Жабдықтың сипаттары терезесінде, **Корпоративтік құрылғылар** бөлімінде құрылғыға *Корпоративтік* белгісін беру тәсілін таңдаңыз:

   - **Құрылғы үшін корпоративтік құрылғы атрибутын қолмен орнату**. *Корпоративтік кластың аппараттық жасақтамасы* белгісі құрылғыға **Жалпы** бөліміндегі құрылғы сипаттары терезесінде қолмен тағайындалады.
   - **Құрылғы үшін корпоративтік құрылғы атрибутын автоматты түрде орнату**. **Құрылғы түрі бойынша** параметрлер блогында бағдарлама *Корпоративтік* белгісін автоматты түрде тағайындайтын құрылғылардың түрлерін көрсетіңіз.

     Бұл параметр желі сауалнамасы арқылы қосылған құрылғыларға ғана әсер етеді. Қолмен қосылған құрылғылар үшін *Корпоративтік* параметрін қолмен орнатыңыз.
4. **OK** түймесін басыңыз.

Корпоративтік құрылғыларды анықтау критерийлері конфигурацияланған.

Пайдаланушы өрістерін конфигурациялау

Пайдаланушы өрістерін конфигурациялау үшін:

1. **Қоймалар** қалтасындағы консоль шежіресінен **Жабдық** салынған қалтасын таңдаңыз.
2. **Жабдық** қалтасының жұмыс аймағында **Қосымша әрекеттер** түймесін басып, ашылмалы тізімнен **Пайдаланушылық деректер өрістерін теңшеу** тармағын таңдаңыз.

   Жабдық сипаттары терезесі ашылады.
3. Жабдық сипаттары терезесінде, **Пайдаланушы өрістері** бөлімінде **Қосылуда** түймесін басыңыз.

   Өріс қосу терезесі ашылады.
4. **Өріс қосу** терезесінде жабдықтың сипаттарында көрсетілетін пайдаланушы өрісі атауын көрсетіңіз.

   Сіз бірегей атауы бар бірнеше пайдаланушы өрістерін жасай аласыз.
5. **OK** түймесін басыңыз.

Нәтижесінде, **Пайдаланушы өрістері** бөліміндегі жабдық сипаттарында қосылған пайдаланушы өрістері көрсетілетін болады. Сіз құрылғылар туралы айрықша ақпаратты көрсету үшін пайдаланушы өрістері қолдана аласыз. Мысалы, жабдықты сатып алуға арналған ішкі өтінімнің нөмірі.

Бағдарламаны лицензиялау

Бұл бөлімде Kaspersky Security Center 15.1 лицензиялаумен байланысты негізгі түсініктер туралы ақпарат бар.

Лицензия шектеуден асып кету оқиғалары

Kaspersky Security Center, клиент құрылғыларында орнатылған Kaspersky бағдарламаларының лицензия шектеулерінен асып кету оқиғалары туралы ақпарат алуға мүмкіндік береді.

Лицензия шектеуден асып кету туралы оқиғалардың маңыздылық деңгейі мынадай ережелер бойынша айқындалады:

- Бір лицензияның пайдаланылатын лицензиялық бірліктерінің саны осы лицензияның лицензиялық бірліктерінің жалпы санының 90%–100% аралығында болса, **Ақпараттық хабарлар** маңыздылық деңгейі бар оқиға жарияланады.
- Бір лицензияның пайдаланылатын лицензиялық бірліктерінің саны осы лицензияның лицензиялық бірліктерінің жалпы санының 100%–110% аралығында болса, **Ескерту** маңыздылық деңгейі бар оқиға жарияланады.
- Бір лицензияның пайдаланылатын лицензиялық бірліктерінің саны осы лицензияның лицензиялық бірліктерінің жалпы санының 110%-нан асатын болса, **Критикалық оқиға** маңыздылық деңгейі бар оқиға жарияланады.

Лицензиялау туралы

Бұл бөлімде Kaspersky Security Center арқылы басқарылатын Kaspersky бағдарламаларын лицензиялау туралы мәліметтер қамтылған.

Лицензия туралы

Лицензия – Лицензиялық келісім негізінде сізге Kaspersky Security Center берілген бағдарламаны пайдалану уақыты шектелген құқық.

Көрсетілетін қызметтердің көлемі және қолданбаны пайдалану мерзімі қолданба қолданылатын лицензияға байланысты.

Лицензиялардың келесі түрлері қарастырылған:

- *Сынақ*.

  Бағдарламамен танысуға арналған тегін лицензия. Сынақ лицензиясының жарамдылық мерзімі қысқа.

Сынақ лицензиясының мерзімі аяқталғаннан кейін, Kaspersky Security Center бағдарламасы өзінің барлық функцияларын орындауды тоқтатады. Қолданбаның пайдалануды жалғастыру үшін сізге коммерциялық лицензия сатып алу қажет.

Бағдарламаны сынақ лицензиясы бойынша тек бір сынақ мерзімінде пайдалануға болады.

- *Коммерциялық.*

  Ақылы лицензия.

  Коммерциялық лицензияның қолданылу мерзімі аяқталғаннан кейін, бағдарлама өзінің негізгі функцияларын орындауды тоқтатады. Kaspersky Security Center бағдарламасын пайдалануды жалғастыру үшін коммерциялық лицензияның жарамдылық мерзімін ұзарту қажет. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, бағдарламаны енді пайдалана алмайсыз және оны құрылғыңыздан жоюыңыз керек.

  Компьютерлік қауіпсіздік қатерлерінен үздіксіз қорғауды қамтамасыз ету үшін лицензияның жарамдылық мерзімін оның аяқталу күнінен кешіктірмей ұзарту ұсынылады.

Лицензиялық келісім туралы

Лицензиялық келісім – бағдарламаны қандай шарттарда пайдалана алатыныңыз көрсетілген, сіз бен АО "Лаборатория Касперского" арасында жасалған заңды келісім.

Қолданбамен жұмыс істемей тұрып, Лицензиялық келісім шарттарын мұқият оқыңыз.

Kaspersky Security Center және оның құрамдастары, мысалы, Желілік агент, өздерінің Лицензиялық келісімдеріне ие.

Сіз Kaspersky Security Center үшін Лицензиялық келісімнің шарттарымен келесі тәсілдер арқылы таныса аласыз:

- Kaspersky Security Center орнату кезінде.
- Kaspersky Security Center жеткізу жиынтығына қосылған license.txt құжатын оқығаннан кейін.
- Kaspersky Security Center орнату қалтасындағы license.txt құжатын оқығаннан кейін.
- Kaspersky сайтынан license.txt файлын жүктеп алу арқылы.

Сіз Windows үшін Желілік агент, Mac үшін Желілік агент және Linux үшін Желілік агент үшін Лицензиялық келісімнің шарттарын келесі жолдармен тексере аласыз:

- Желілік агенттің дистрибутивін Kaspersky веб-серверлерінен жүктеу кезінде.
- Windows үшін Желілік агент, Mac үшін Желілік агент және Linux үшін Желілік агент дистрибутивін орнатқан кезде.
- Windows үшін Желілік агент, Mac үшін Желілік агент немесе Linux үшін Желілік агент дистрибутивінің бөлігі болып табылатын license.txt құжатын оқығаннан кейін.
- Windows үшін Желілік агент, Mac үшін Желілік агент немесе Linux үшін Желілік агенттің орнату қалтасындағы license.txt құжатын оқығаннан кейін.
- Kaspersky сайтынан license.txt файлын жүктеп алу арқылы.

Сіз бағдарламаны орнату кезінде Лицензиялық келісімнің мәтінімен келіскеніңізді растай отырып, Лицензиялық келісімнің шарттарын қабылдайсыз. Егер сіз Лицензиялық келісімнің шарттарымен келіспесеңіз, бағдарламаны орнатуды тоқтатып, бағдарламаны пайдаланбауыңыз керек.

Лицензиялық сертификат туралы

Лицензиялық сертификат – бұл кілт файлы немесе белсендіру кодымен бірге сізге берілетін құжат.

Лицензиялық сертификатта, ұсынылатын лицензия туралы келесі ақпарат бар:

- Лицензия идентификаторы немесе тапсырыс нөмірі
- Лицензия берілетін пайдаланушы туралы ақпарат
- Берілетін лицензия бойынша белсендіруге болатын бағдарлама туралы ақпарат
- Лицензиялау бірліктерінің санына қойылатын шектеу (мысалы, берілетін лицензия бойынша бағдарламаны пайдалануға болатын құрылғылар)
- Лицензияның қолданылу мерзімі басталған күн
- Лицензияның жарамдылық мерзімінің аяқталу күні немесе лицензияның қолданылу мерзімі
- Лицензия түрі

Лицензиялық кілт туралы

Лицензиялық кілт – Лицензиялық келісім шарттарына сәйкес бағдарламаны белсендіріп, пайдалануға мүмкіндік беретін биттер тізбегі. Лицензиялық кілтті Kaspersky мамандары жасайды.

Бағдарламаға лицензиялық кілтті келесі тәсілдердің бірімен қосуға болады: *кілт файлын* қолдану немесе *белсендіру кодын* енгізу. Лицензиялық кілт бағдарламаның интерфейсінде, оны бағдарламаға қосқаннан кейінгі бірегей әріптік-цифрлық реттілік түрінде көрсетіледі.

Лицензиялық келісімнің шарттары бұзылған жағдайда, лицензиялық кілтті Kaspersky бұғаттауы мүмкін. Егер лицензиялық кілт бұғатталған болса, бағдарлама жұмыс істеуі үшін басқа лицензиялық кілтті қосу қажет.

Лицензиялық кілт белсенді және қосымша (резервтік) болуы мүмкін.

Белсенді лицензиялық кілт – ағымдағы сәтте бағдарламаның жұмыс істеуі үшін қолданылатын лицензиялық кілт. Белсенді кілт ретінде, сынақ немесе коммерциялық лицензия үшін лицензиялық кілтті қосуға болады. Бағдарламада бірден артық белсенді лицензиялық кілт болуы мүмкін емес.

Қосымша (резервттегі) лицензиялық кілт – бағдарламаны қолдану құқығын растайтын, бірақ ағымдағы сәтте қолданылмайтын лицензиялық кілт. Ағымдағы белсенді лицензиялық кілтпен байланысты лицензияның мерзімі аяқталғалы жатқан кезде қосымша лицензиялық кілт автоматты түрде белсенді болады. Қосымша лицензиялық кілтті тек белсенді лицензиялық кілт болған жағдайда ғана қосуға болады.

Сынақ лицензиясының лицензиялық кілті тек белсенді лицензиялық кілт ретінде қосылуы мүмкін. Сынақ лицензиясының лицензиялық кілтін қосымша лицензиялық кілт ретінде қосу мүмкін емес.

Кілт файлы туралы

Кілт файлы – Kaspersky сізге ұсынатын key кеңейтімі бар файл. Кілт файлы бағдарламаны белсендіретін лицензиялық кілтті қосуға арналған.

Сіз Kaspersky Security Center бағдарламасын сатып алғаннан немесе Kaspersky Security Center сынақ нұсқасына тапсырыс бергеннен кейін, өзіңіз көрсеткен электрондық пошта мекенжайы бойынша кілт файлын аласыз.

Бағдарламаны кілт файлы арқылы белсендіру үшін Kaspersky белсендіру серверлеріне қосылудың қажет емес.

Егер кілт файлы кездейсоқ жойылса, оны қалпына келтіруге болады. Сізге кілт файлы қажет болуы мүмкін, мысалы, Kaspersky CompanyAccount порталында тіркелу үшін.

Кілт файлын қалпына келтіру үшін келесі әрекеттердің бірін орындау керек:

- Лицензия сатушысына хабарласу.
- Қолда бар белсендіру коды негізінде Kaspersky веб-сайтынан кілт файлын алу.
- Басқа басқару серверінен кілт файлын экспорттау.

Жазылым туралы

Kaspersky Security Center-ге жазылым – бұл параметрлері таңдалған бағдарламаны қолдануға тапсырыс беру (жазылымның аяқталу күні, қорғалатын құрылғылардың саны). Kaspersky Security Center-ге жазылымды провайдерде (мысалы, интернет-провайдерде) тіркеуге болады. Жазылымды қолмен немесе автоматты режимде ұзартуға немесе одан бас тартуға болады.

Жазылым шектеулі (мысалы, бір жылға) немесе шектеусіз (аяқталу күні жоқ) болуы мүмкін. Шектеулі жазылым аяқталғаннан кейін Kaspersky Security Center жұмысын жалғастыру үшін, оны жаңарту қажет. Провайдерге алдын ала төлем уақтылы енгізілген жағдайда, шектеусіз жазылым автоматты түрде ұзартылады.

Егер жазылым шектеулі болса, жазылым аяқталғаннан кейін жазылымды ұзарту үшін жеңілдік кезеңі берілуі мүмкін, оның барысында бағдарламаның функционалдығы сақталады. Жеңілдік кезеңінің болуы мен ұзақтығын провайдер айқындайды.

Kaspersky Security Center жазылымын пайдалану үшін провайдер ұсынған белсендіру кодын қолдану қажет.

Жазылым аяқталғаннан немесе одан бас тартқаннан кейін ғана Kaspersky Security Center пайдалану үшін басқа белсендіру кодын қолдануға болады.

Провайдерге байланысты жазылымды басқаруға арналған ықтимал әрекеттер жиынтығы әртүрлі болуы мүмкін. Провайдер бағдарламаның функционалдығы сақталатын жазылымның мерзімін ұзарту үшін жеңілдік кезеңін ұсынбауы мүмкін.

Жазылым арқылы сатып алынған белсендіру кодтарын Kaspersky Security Center бағдарламасының алдыңғы нұсқаларын белсендіру үшін пайдалану мүмкін емес.

Жазылым бағдарламасын пайдалану кезінде, Kaspersky Security Center бағдарламасы автоматты түрде белсендіру серверіне жазылымның аяқталу күніне дейін белгілі бір уақыт аралығында жүгінеді. Бұл жазылым туралы ақпаратты белсендіру серверімен синхрондауды қамтамасыз етеді. Жүйелік DNS арқылы серверге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Сіз жазылымды провайдердің веб-сайтында ұзарта аласыз.

Жазылым туралы ақпаратты, Kaspersky Security Center белсендіру серверіне қатынас алуын күтпей-ақ, қолмен де жаңартуға болады. Мысалы, бұл жазылым параметрлерін өзгерту кезінде пайдалы болуы мүмкін.

Жазылым туралы ақпаратты қолмен жаңарту үшін:

1. Консоль ағашында **Kaspersky лицензиялары"** қалтасын таңдаңыз.
2. **Қосымша әрекеттер** түймесін басып, ашылмалы тізімнен **Жазылым параметрлерін Лицензия серверімен синхрондау** нұсқасын таңдаңыз.

Жазылым туралы ақпарат белсендіру серверінде жаңартылды.

Белсендіру коды туралы

Белсендіру коды – жиырма латын әрпі мен санынан құралған бірегей бірізділік. Сіз Kaspersky Security Center бағдарламасын белсендіретін лицензиялық кілтті қосу үшін белсендіру кодын енгізесіз. Сіз Kaspersky Security Center бағдарламасын сатып алғаннан немесе Kaspersky Security Center сынақ нұсқасына тапсырыс бергеннен кейін, өзіңіз көрсеткен электрондық пошта мекенжайы бойынша белсендіру кодын аласыз.

Бағдарламаны белсендіру кодының көмегімен белсендіру үшін, Kaspersky белсендіру серверлеріне қосылу мақсатында интернетке қатынасу талап етіледі. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Бағдарлама белсендіру кодының көмегімен белсендірілген болса, белсендіруден кейін кейбір жағдайларда, бағдарлама лицензиялық кілттің ағымдағы күйін тексеру үшін Kaspersky белсендіру серверлеріне үнемі сұраулар жіберіп тұрады. Сұраулар жіберу үшін бағдарламаға интернетке қатынасу мүмкіндігін ұсыну керек.

Бағдарламаны орнатқаннан кейін белсендіру кодын жоғалтып алсаңыз, сізге лицензияны сатқан Kaspersky серіктесімен хабарласыңыз.

> Сіз басқарылатын бағдарламаларды белсендіру үшін кілт файлдарын қолдана алмайсыз; сіз тек белсендіру кодтарын ғана қолдана аласыз.

Лицензиялық келісімге берілген келісімді кері қайтарып алу

Егер сіз клиент құрылғыларын қорғауды тоқтатуды шешсеңіз, Kaspersky басқарылатын бағдарламаларын жойып, осы бағдарламалар үшін Лицензиялық келісімді алып тастай аласыз.

Kaspersky басқарылатын бағдарламалары үшін Лицензиялық келісімді кері қайтарып алу үшін:

1. Консоль ағашында **Басқару сервері** → **Қосымша** → **Қабылданған Лицензиялық келісімдер** тармағын таңдаңыз.

   Орнату пакеттерін жасау, жаңартуларды орнату немесе Kaspersky Security for Mobile қолданбасын орналастыру кезінде қабылданған Лицензиялық келісімдердің тізімі көрсетіледі.

2. Тізімнен қайтарып алғыңыз келетін Лицензиялық келісімдерді таңдаңыз.

   Лицензиялық келісімдердің келесі сипаттарын көруге болады:

   - Лицензиялық келісімді қабылдау күні.
   - Лицензиялық келісімді қабылдаған пайдаланушы аты.
   - Лицензиялық келісімнің шарттарына сілтеме.
   - Лицензиялық келісім қолданылатын нысандардың тізімі: орнату пакеттерінің атаулары, жаңарту атаулары, ұялы қолданбалардың атаулары.

3. **Лицензиялық келісімді қайтару** түймесін басыңыз.

   Ашылған терезеде осы Лицензиялық келісімге сәйкес келетін Kaspersky бағдарламасын жою қажет екендігі туралы ақпарат көрсетіледі.

4. Лицензияны қайтарып алуды растайтын түймесін басыңыз.

   Kaspersky Security Center бағдарламасы, Лицензиялық келісімін қайтарып алынатын Kaspersky басқарылатын бағдарламасына сәйкес келетін орнату пакеттерінің жойылғанын тексереді.

   Орнату пакеті жойылған Kaspersky басқарылатын бағдарламасы үшін Лицензиялық келісімді ғана қайтарып алуға болады.

Лицензиялық келісім қайтарып алынды. Ол **Басқару сервері → Қосымша → Қабылданған Лицензиялық келісімдер** бөліміндегі Лицензиялық келісімдер тізімінде көрсетілмейді. Лицензиялық келісімі қайтарып алынған Kaspersky бағдарламасын енді клиент құрылғыларын қорғау үшін пайдалану мүмкін емес.

Деректерді беру туралы

Үшінші тараптарға берілетін деректер

Android операциялық жүйесі іске қосылған құрылғыларға push хабарландыру механизмі арқылы пәрмендерді уақтылы жеткізу мақсатына бағдарламалық жасақтаманың мобильдік құрылғыны басқару функциясын пайдаланған кезде, Google Firebase Cloud Messaging қызметі қолданылады. Пайдаланушы Google Firebase Cloud Messaging қызметін пайдалануды конфигурациялаған болса, Пайдаланушы келесі ақпаратты Google Firebase Cloud Messaging қызметіне автоматты режимде ұсынуға келіседі: push хабарландырулары жіберілуі керек Kaspersky Endpoint Security for Android бағдарламаларын орнату идентификаторлары.

Google Firebase Cloud Messaging қызметімен ақпарат алмасуды бұғаттау үшін, Пайдаланушы Google Firebase Cloud Messaging қызметін пайдалану конфигурацияларын бастапқы мәнге келтіруі керек.

iOS операциялық жүйесі іске қосылған құрылғыларға push хабарландыру механизмі арқылы пәрмендерді уақтылы жеткізу мақсатына бағдарламалық жасақтаманың мобильдік құрылғыны басқару функциясын пайдаланған кезде, Apple Push Notification Service (APN) қызметі қолданылады. Егер Пайдаланушы iOS MDM серверіне APNs сертификатын орнатқан болса, iOS ұялы құрылғыларын Бағдарламалық жасақтамаға қосу параметрлерінің жиынтығымен iOS MDM профилін қалыптастырса және осы iOS MDM профилін ұялы құрылғыларға орнатса, Пайдаланушы автоматты режимде APNs сервисіне келесі ақпаратты ұсынуға келіседі:

- Токен – құрылғының push-токені. Сервер құрылғыға push хабарландыруларын жіберген кезде осы токенді пайдаланады.
- PushMagic – push хабарландыруына қосылуы керек жол. Жолдың мәні құрылғы арқылы жасалады.

Жергілікті түрде өңделетін деректер

Kaspersky Security Center бағдарламасы ұйымның желісін қорғау жүйесін басқару және қызмет көрсету жөніндегі негізгі тапсырмаларды орталықтандырылған шешуге арналған. Kaspersky Security Center әкімшіге ұйым желісінің қауіпсіздік деңгейі туралы егжей-тегжейлі ақпаратқа қатынасуға мүмкіндік береді және Kaspersky бағдарламалары негізінде құрылған қорғаныстың барлық құрамдастарын конфигурациялауға мүмкіндік береді. Kaspersky Security Center келесі негізгі функцияларды орындайды:

- Ұйымның желісінде құрылғылар мен олардың пайдаланушыларын анықтау
- Құрылғыларды басқару үшін басқару топтарының иерархиясын қалыптастыру
- Құрылғыларға Kaspersky бағдарламаларын орнату
- Орнатылған бағдарламалардың жұмыс параметрлері мен тапсырмаларын басқару
- Kaspersky және басқа өндірушілер бағдарламаларының жаңартуларын басқару, осалдықтарды іздеу және түзету
- Құрылғыларда Kaspersky бағдарламаларын белсендіру
- Пайдаланушы есептік жазбаларын басқару
- Құрылғылардағы Kaspersky бағдарламаларының жұмысы туралы ақпаратты қарау
- Есептерді қарау

Өзінің негізгі функцияларын орындау үшін Kaspersky Security Center бағдарламасы келесі ақпаратты қабылдай алады, сақтай алады және өңдей алады:

- Ұйым желісіндегі құрылғылар туралы ақпарат Windows, Active Directory немесе Samba домен контроллерлеріне сауалнама жүргізу немесе IP ауқымдарына сауалнама жүргізу арқылы алынады. Басқару серверінің өзі деректерді қабылдайды немесе оларды оған тарату нүктесі рөлін атқаратын желілік агент жібереді.
- Ұйымдық бөлімшелер, домендер, пайдаланушылар және топтар туралы Active Directory және Samba ақпараты. Басқару серверінің өзі деректерді қабылдайды немесе оларды оған тарату нүктесі рөлін атқаратын желілік агент жібереді.

- Басқарылатын құрылғылар туралы деректер. Желілік агент құрылғыдан Басқару серверіне төменде келтірілген деректерді жібереді. Пайдаланушы құрылғының көрсетілетін атауы мен сипаттамасын Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console интерфейсіне енгізеді:

  - Құрылғыны анықтау үшін қажетті басқарылатын құрылғы мен оның құрамдастарының техникалық сипаттамалары, яғни құрылғының көрсетілетін атауы мен сипаттамасы, атауы мен түрі (Windows доменіне тиесілі құрылғылар үшін), ортадағы құрылғы атауы (Windows доменіне тиесілі құрылғылар үшін), DNS домені және DNS атауы, IPv4 мекенжайы, IPv6 мекенжайы, желілік орналасуы, MAC мекенжайы, сериялық нөмірі, операциялық жүйенің түрі, құрылғының виртуалды машина болып табылатыны және гипервизор түрі, құрылғының VDI бөлігі ретінде динамикалық виртуалды машина болып табылатыны.

  - Басқарылатын құрылғылардың аудиті үшін және қандай да бір патчтар мен жаңартуларды қолдануға болатыны туралы шешім қабылдау үшін қажетті басқарылатын құрылғылар мен олардың құрамдастарының басқа да сипаттамалары: Windows жаңартулар агентінің (WUA) күйі, операциялық жүйенің архитектурасы, операциялық жүйені жеткізуші, операциялық жүйе құрастырылымы, операциялық жүйе шығарылымының идентификаторы, операциялық жүйе орналасқан қалта, егер құрылғы виртуалды машина болса, онда виртуалды машинаның түрі; құрылғылар басқаратын виртуалды Басқару серверінің атауы; бұлтты құрылғы туралы деректер (бұлтты аймақ, VPC, бұлтты қолжетімділік аймағы, бұлтты қосалқы желісі, бұлтты құрылғыны орналастыру тобы).

  - Басқарылатын құрылғылардағы әрекеттер туралы егжей-тегжейлі деректер: соңғы рет жаңартылған күні мен уақыты, құрылғы желіде соңғы рет көрінген уақыт, қайта іске қосуды күту күйі, құрылғыны қосу уақыты.

  - Құрылғылардың пайдаланушыларының есептік жазбалары және олардың жұмыс сеанстары туралы деректер.

- Басқарылатын құрылғыда қашықтағы диагностиканы іске қосу кезінде алынған деректер: трассалау файлдары, жүйелік ақпарат, құрылғыда орнатылған Kaspersky қолданбасы туралы ақпарат, дамп файлдары, оқиғалар журналдары, Kaspersky техникалық қолдау қызметінен алынған диагностикалық скриптілерді іске қосу нәтижелері.

- Егер құрылғы тарату нүктесі болса, тарату нүктесінің жұмыс статистикасы. Желілік агент деректерді құрылғыдан Басқару серверіне жібереді.

- Пайдаланушы Басқару консольдеріне немесе Kaspersky Security Center Web Console жүйесіне енгізетін тарату нүктесінің параметрлері.

- Ұялы құрылғыларды Басқару серверіне қосу үшін қажетті деректер: сертификат, ұялы құрылғыларды қосу порты, Басқару серверіне қосылу мекенжайы. Пайдаланушы деректерді Басқару консольдеріне Kaspersky Security Center Web Console веб-консоліне енгізеді.

- iOS MDM протоколы бойынша жіберілетін ұялы құрылғылар туралы деректер. Төменде атап көрсетілген деректер ұялы құрылғыдан Басқару серверіне беріледі:

  - Құрылғыны анықтау үшін қажетті ұялы құрылғы мен оның құрамдастарының техникалық сипаттамалары: құрылғының атауы, үлгісі, атауы және операциялық жүйе құрастырылымы, құрылғы үлгісі нөмірі, IMEI, UDID, MEID нөмірі, сериялық нөмірі, жад көлемі, модем шағын бағдарламасының нұсқасы, Bluetooth MAC мекенжайы, Wi-Fi MAC мекенжайы және SIM картасының деректері (SIM картасы идентификаторының бөлігі ретіндегі ICCID коды).

  - Ұялы құрылғы пайдаланатын ұялы байланыс желісі туралы деректер: ұялы байланыс желісінің түрі, пайдаланылатын ұялы байланыс желісінің атауы, үйдегі ұялы байланыс желісінің атауы, ұялы байланыс желісі операторы параметрлерінің нұсқасы, дауыстық роуминг және деректер роумингі күйі, үй желісіне арналған ел коды, орналасу елінің коды, пайдаланылатын желінің ел коды және шифрлау деңгейі.

- Ұялы құрылғының қауіпсіздік параметрлері: құпиясөзді пайдалану және оны саясат параметрлеріне сәйкес келуі, конфигурациялық профильдер және үшінші тарап қолданбаларын орнату үшін пайдаланылатын provisioning профильдері тізімі.

- Басқару серверімен соңғы рет синхрондау күні және құрылғыны басқару күйі.

- Құрылғыда орнатылған Kaspersky бағдарламалары туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді:

  - Басқарылатын құрылғыда орнатылған Kaspersky бағдарламаларының параметрлері: Kaspersky бағдарламасының атауы мен нұсқасы, күйі, тұрақты қорғау күйі, құрылғыны соңғы тексеру күні мен уақыты, анықталған қауіптер саны, зарарсыздандыру орындалмаған нысандар саны, бағдарлама компоненттерінің болуы және күйі, антивирустық дерекқорлардың соңғы рет жаңартылған уақыты мен нұсқасы, Kaspersky бағдарламасының параметрлері мен тапсырмалары туралы ақпарат, белсенді және резеревтегі лицензиялық кілттер туралы ақпарат, бағдарламаны орнату күні мен идентификаторы.

  - Бағдарлама жұмысының статистикасы: басқарылатын құрылғыдағы Kaspersky бағдарламасының құрамдастары күйінің өзгерістерімен және бағдарламалық құрамдастар бастаған тапсырмаларды орындаумен байланысты оқиғалар.

  - Kaspersky бағдарламасы айқындаған құрылғының күйі.

  - Kaspersky бағдарламасы беретін тегтер.

  - Kaspersky бағдарламасына орнатылған және қолданылатын жаңартулар жиынтығы.

- Kaspersky Security Center құрамдастары және Kaspersky басқарылатын бағдарламалары оқиғаларында қамтылған деректер. Желілік агент деректерді құрылғыдан Басқару серверіне жібереді.

- Kaspersky Security Center бағдарламасын оқиғаларды экспорттауға арналған SIEM жүйесімен біріктіру үшін қажетті деректер. Пайдаланушы деректерді Басқару консольдеріне Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Саясат және саясат профильдері түрінде ұсынылған Kaspersky Security Center құрамдастарының және Kaspersky басқарылатын бағдарламаларының конфигурациялары. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Kaspersky Security Center құрамдастары және Kaspersky басқарылатын бағдарламалары тапсырмаларының конфигурациялары. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Осалдықтар мен патчтарды басқару функциясы өңдейтін деректер. Желілік агент құрылғыдан Басқару серверіне төменде келтірілген деректерді жібереді:

  - Басқарылатын құрылғыларда орнатылған бағдарламалар мен патчтар туралы деректер (Бағдарламалар тізімдемесі).

  - Басқарылатын құрылғыларда табылған жабдық туралы ақпарат (Жабдық тізімдемесі).

    Желілік агент Windows жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді:

    - ЖЖҚ

    - Жаппай сақтау құрылғылары

    - Негізгі тақта

- Процессор
- Желілік адаптерлер
- Мониторлар
- Бейне адаптері
- Дыбыстық карта

Желілік агент Linux немесе macOS жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді (бұл ақпаратты операциялық жүйе қамтамасыз етсе):

- Жалпы ЖЖҚ көлемі
- Жаппай сақтау құрылғыларының жалпы көлемі
- Негізгі тақта
- Процессор
- Желілік адаптерлер

- Басқарылатын құрылғыларда анықталған үшінші тарап бағдарламалық жасақтамасының осалдықтары туралы деректер.
- Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламалары үшін қолжетімді жаңарту туралы деректер.
- WSUS функциясы тапқан Microsoft жаңартулары туралы деректер.
- Құрылғыға орнатылуы тиісті WSUS функциясы тапқан Microsoft жаңартуларының тізімі.

- Басқарылатын құрылғылардағы үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін жаңартуларды оқшауланған Басқару серверіне жүктеу үшін қажетті деректер. Пайдаланушы Басқару серверінің klscflag утилитасын пайдаланып, деректерді енгізеді және жібереді.
- Kaspersky Security Center бағдарламасының бұлтты ортамен (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud) жұмыс істеуі үшін қажетті деректер. Пайдаланушы деректерді Басқару консольдеріне Kaspersky Security Center Web Console веб-консоліне енгізеді.
- Реттелмелі бағдарламалар санаттары. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.
- Бағдарламаны басқару функциясы арқылы басқарылатын құрылғыларда анықталған орындалатын файлдар туралы деректер. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді. Деректердің толық тізімі тиісті қолданбаның анықтамасында келтірілген.
- Сақтық көшірмелеуге орналастырылған файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Карантинге орналастырылған файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Егжей-тегжейлі талдау үшін Kaspersky мамандары сұраған файлдар туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Аномалияларды бейімделумен басқару ережелерінің күйі және іске қосылуы туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Басқарылатын құрылғыға орнатылған немесе қосылған және Құрылғыны басқару функциясы анықтаған сыртқы құрылғылар (жад құрылғылары, ақпаратты беру құралдары, ақпаратты қатты көшірмеге айналдыру құралдары, қосылым шиналары) туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Шифрленген құрылғыларды шифрлау және шифрлау күйі туралы ақпарат. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді.

- Kaspersky бағдарламаларының деректерін шифрлау функциясы орындайтын құрылғылардағы деректерді шифрлау қателері туралы деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Басқарылатын бағдарламаланатын логикалық контроллерлер (БЛК) тізімі. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Қауіптердің даму тізбегін жасауға арналған деректер. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Ұйым қызметкерлерінің бұлттық сервистерге қол жеткізу әрекеттері туралы ақпарат. Басқарылатын бағдарлама деректерді құрылғыдан Басқару серверіне Желілік агент арқылы жібереді. Деректердің толық тізімі тиісті бағдарламаның анықтамасында келтірілген.

- Kaspersky Security Center бағдарламасын Kaspersky Managed Detection and Response қызметімен біріктіруге қажетті деректер (Kaspersky Security Center Web Console үшін арнайы плагин орнатылуы тиіс): біріктіруді бастау токені, біріктіру токені және пайдаланушы сеансы токені. Пайдаланушы біріктіруді бастау токені арқылы Kaspersky Security Center Web Console интерфейсіне кіреді. Kaspersky MDR қызметі арнайы плагин арқылы біріктіру токенін және пайдаланушы сеансы токенін береді.

- Енгізілген белсендіру кодтары немесе көрсетілген кілт файлдары туралы толық ақпарат. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Пайдаланушылардың есептік жазбалары: атауы, сипаттамасы, толық атауы, электрондық пошта мекенжайы, негізгі телефон нөмірі, құпиясөзі, Басқару сервері жасаған құпия кілті және екі қадамдық тексеру үшін бір реттік құпиясөз. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Есептік деректер және қатынасу диспетчеріне Kaspersky Security Center бағдарламасымен біріктірілген Kaspersky бағдарламалары арасында бірыңғай кіруді (SSO) қамтамасыз ету үшін және орталықтандырылған түпнұсқалық растама үшін қажетті деректер: Есептік деректер және қатынасу диспетчерін орнату және конфигурациялау параметрлері, Есептік деректер және қатынасу диспетчері токендері, клиент бағдарламалары күйлері және ресурс серверлері күйлері. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Басқару нысандарының тексерістер журналы. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Пайдаланушы тексеріс жасаған құрылғының IP мекенжайы. IP мекенжайын Басқару сервері автоматты түрде анықтайды.

- Жойылған басқару нысандары тізімдемесі. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Файлдан жасалған орнату пакеттері және орнату параметрлері. Пайдаланушы деректерді Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізеді.

- Kaspersky хабарландыруларын Kaspersky Security Center Web Console веб-консолінде көрсетуге қажетті деректер. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Kaspersky Security Center Web Console веб-консолінде басқарылатын бағдарлама плагиндерінің жұмыс істеуі үшін қажетті және күнделікті жұмыс барысында Басқару сервері дерекқорында плагиндер сақтайтын деректер. Сипаттама және деректерді беру тәсілдері тиісті бағдарламаның анықтама файлдарында келтірілген.

- Kaspersky Security Center Web Console пайдаланушы конфигурациялары: локализация тілі және пайдаланушы интерфейсі тақырыбы, бақылау тақтасын көрсету конфигурациялары, нотификациялар күйі туралы ақпарат (оқылған/оқылмаған), кестелердегі бағандардың күйі (жасыру/көрсету), оқу режимінің өту барысы. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Kaspersky Security Center құрамдастары мен Kaspersky басқарылатын құрылғыларына арналған Kaspersky Event журналы. Kaspersky Event Log оқиғалар журналы құрылғыда сақталады және Басқару серверіне ешқашан берілмейді.

- Басқарылатын құрылғыларды Kaspersky Security Center құрамдастарына қауіпсіз қосу сертификаты. Пайдаланушы деректерді басқару серверінің klsetsrvcert утилитасы көмегімен енгізеді.

- Ұйымның ішкі веб-ресурстарына сенім орнатуға арналған сертификаттар. Пайдаланушы деректерді Kaspersky Security Center Web Console интерфейсінде енгізеді.

- Kaspersky Security Center бағдарламасының Amazon Web Services (AWS), Microsoft Azure, Google Cloud және Yandex.Cloud сияқты бұлтты орталарда жұмыс істеуі үшін қажетті деректер. Басқару сервері деректерді іске қосылып тұрған виртуалды машинадан алады.

- Пайдаланушының Kaspersky ұйымымен жасалған заңды келісімдерді қабылдауы туралы ақпарат.

- Пайдаланушы келесі құрамдастарға енгізетін Басқару сервері деректері:

  - Басқару консолі

  - Kaspersky Security Center Web Console

    - klscflag утилитасын қолдану кезінде пәрмен жолы терминалы
    - klakaut және OpenAPI Kaspersky Security Center автоматтандыру нысандары арқылы Басқару серверімен өзара әрекеттесетін құрамдастар
- Пайдаланушы Басқару консолі интерфейсіне немесе Kaspersky Security Center Web Console веб-консоліне енгізетін кез келген деректер.

Жоғарыда атап көрсетілген деректер Kaspersky Security Center бағдарламасына келесі тәсілдермен кіруі мүмкін:

- Пайдаланушы деректерді келесі құрамдастардың интерфейсіне енгізеді:
    - Басқару консолі
    - Kaspersky Security Center Web Console
    - klscflag утилитасын қолдану кезінде пәрмен жолы терминалы
    - klakaut және OpenAPI Kaspersky Security Center автоматтандыру нысандары арқылы Басқару серверімен өзара әрекеттесетін құрамдастар
- Желілік агент құрылғыдан деректерді өз бетінше алады және Басқару серверіне жібереді.
- Желілік агент Kaspersky бағдарламасы арқылы жиналған деректерді алады және Басқару серверіне жібереді. Kaspersky басқарылатын бағдарламалары өңдейтін деректер тізбесі тиісті бағдарламалардың анықтамаларында келтірілген.
- Басқару сервері желілік құрылғылар туралы ақпаратты өз бетінше алады немесе оны тарату нүктесі ретінде әрекет ететін желілік агент жібереді.
- Деректер мобильдік құрылғыдан басқару серверіне iOS MDM протоколы арқылы беріледі.

Атап көрсетілген деректер Басқару сервері дерекқорында сақталады. Пайдаланушы аттары және құпиясөздер шифрланған түрде сақталады.

Жоғарыда аталған барлық деректерді Kaspersky бағдарламасына тек Kaspersky Security Center құрамдастарының қоқыс файлдары, трассалау файлдары немесе журнал файлдары, соның ішінде инсталляторлар мен утилиталар жасайтын журналдар файлдары арқылы беруге болады.

Kaspersky Security Center құрамдастарының қоқыс файлдары, трассалау файлдары және журнал файлдары басқару серверінің, желілік агенттің, басқару консолінің, iOS MDM серверінің, Kaspersky Security Center Web Console веб-консолінің кездейсоқ деректерін қамтиды. Бұл файлдарда дербес және құпия деректер болуы мүмкін. Қоқыс файлдары, трассалау файлдары және журнал файлдары құрылғыда ашық түрде сақталады. Қоқыс файлдары, трассалау файлдары және журнал файлдары Kaspersky бағдарламасына автоматты түрде берілмейді, алайда, әкімші осы деректерді Kaspersky бағдарламасына Техникалық қолдау қызметінің сұрауы бойынша Kaspersky Security Center жұмысындағы мәселелерді шешу үшін қолмен жібере алады.

Сілтемелер арқылы Басқару консоліне немесе Kaspersky Security Center Web Console веб-консоліне өту арқылы, Пайдаланушы келесі деректерді автоматты түрде жіберуге келіседі:

- Kaspersky Security Center коды
- Kaspersky Security Center нұсқасы
- Kaspersky Security Center локализациясы

- Лицензия идентификаторы
- Лицензия түрі
- Серіктес арқылы лицензияны сатып алу белгісі

Әрбір сілтеме бойынша ұсынылатын деректер тізімі сілтеменің мақсаты мен орналасқан жеріне байланысты.

Kaspersky алынған деректерді жасырын түрде және тек жалпы статистика мақсатында пайдаланады. Жиынтық статистика алынған бастапқы ақпараттан автоматты түрде қалыптастырылады және қандай да бір дербес немесе өзге де құпия деректерді қамтымайды. Жаңа деректер жинақталған кезде алдыңғы деректер жойылады (жылына бір рет). Жиынтық статистика шектелмеген уақыт бойы сақталады.

Kaspersky барлық алынған деректерді заңнамаға және Kaspersky қолданыстағы ережелеріне сәйкес қорғауды қамтамасыз етеді. Деректер қауіпсіз байланыс арналары бойынша беріледі.

Kaspersky Security Center лицензиялау нұсқалары

Kaspersky Security Center келесі режимдерде жұмыс істей алады:

- **Лицензия жоқ (базалық функционалдылық)**

  Kaspersky Security Center, бағдарлама іске қосылғанша немесе коммерциялық лицензияның қолданылу мерзімі аяқталғанға дейін осы режимде жұмыс істейді. Басқару консолінің негізгі функциясын қолдайтын Kaspersky Security Center бағдарламасы ұйымның желісін қорғауға арналған Kaspersky бағдарламаларының құрамында жеткізіледі. Бұдан бөлек, ол Kaspersky веб-сайтынан жүктеу үшін қолжетімді.

- **Коммерциялық лицензия**

  Басқару консолінің базалық функционалдылығына кірмейтін қосымша функционалдылық қажет болса, коммерциялық лицензияны сатып алу қажет.

  Басқару сервері сипаттары терезесіне лицензиялық кілт қосқанда, Kaspersky Security Center пайдалануға мүмкіндік беретін лицензиялық кілтті қосқаныңызға көз жеткізіңіз. Сіз бұл ақпаратты Kaspersky сайтынан таба аласыз. Әрбір шешім бетінде осы шешімге енгізілген бағдарламалардың тізімі бар. Басқару сервері Kaspersky Endpoint Security Cloud лицензия кілті сияқты қолдау көрсетілмейтін лицензия кілттерін қабылдай алады, бірақ мұндай лицензия кілттері Басқару консолінің базалық функционалдылығынан басқа ешқандай жаңа мүмкіндіктерді ұсынбайды.

Функция немесе сипат	Kaspersky Security Center жұмыс режимі	
	Лицензия жоқ	Коммерциялық лицензия
Басқару консолінің негізгі функциясы Келесі функциялар қолжетімді: • Қашықтағы кеңселер немесе ұйым-клиенттер желісін басқару үшін виртуалды Басқару серверлерін құру. • Құрылғылар жиынтығын тұтастай басқару үшін басқару топтарының иерархиясын құру. • Бағдарламаларды қашықтан орнату. • Клиент құрылғыларында орнатылған бағдарлама параметрлерін орталықтандырылған конфигурациялау. • Ұйымның антивирустық қауіпсіздігінің күйін бақылау. • Пайдаланушы рөлдерін басқару. • Бағдарламалардың статистикасы мен есептерін, сондай-ақ критикалық оқиғалар туралы хабарландыруларды алу. • Карантинге немесе сақтық көшірмелеуге орналастырылған файлдармен, сондай-ақ өңделуі кейінге қалдырылған файлдармен орталықтандырылған жұмыс. • Деректерді шифрлау және қорғау процесін басқару. • Қолданыстағы лицензиялы бағдарламалар топтарын қарау және өзгерту. • Желі сауалнамасы нәтижесінде табылған жабдықтар тізімін қолмен қарау және өңдеу. • Қашықтан орнатуға болатын операциялық жүйе кескіндерінің тізімін қарау.	✓	✓
Осалдықтар мен патчтарды басқару: базалық функционалдылық Келесі тапсырмалар коммерциялық лицензияны қажет етпейді: • *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы Осы тапсырмасының көмегімен Kaspersky Security Center бағдарламасы басқарылатын құрылғыларға орнатылған үшінші тарап бағдарламалары үшін табылған осалдықтар мен қажетті жаңартулар тізімдерін алады. • *Windows Update жаңартуларын орнату* тапсырмасы. Бұл тапсырманы тек Windows Update жаңартуларын орнату үшін пайдалануға болады. Бұл тапсырманы пайдалану үшін тапсырма параметрлерінде қажетті жаңартуларды қолмен көрсету керек. • *Осалдықтарды түзету* тапсырмасы *Осалдықтарды түзету* тапсырмасы үшінші тарап бағдарламалары үшін ұсынылған Microsoft бағдарламаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады. Бұл тапсырманы пайдалану мақсатында, тапсырма параметрлерінде осалдықтарды түзету үшін пайдаланушылық түзетулерді қолмен көрсету қажет.	✓	✓
Осалдықтар мен патчтарды басқару: қосымша функционалдылық Келесі функциялар қолжетімді: • Бағдарламалық жасақтама жаңартуларын қашықтан орнату және сіз белгілеген ережелерге сәйкес осалдықтарды автоматты түрде түзету. • Орталықтандырылған режимде және белгіленген аралықтарда құрылғыларда Windows Update қызметтеріне жаңартуларды ұсыну үшін Басқару серверін Windows Server Update Services (WSUS) қызметтерінің сервері ретінде пайдалану.	—	✓

Функция немесе сипат	Kaspersky Security Center жұмыс режимі	
	Лицензия жоқ	Коммерциялық лицензия
ММС негізіндегі Басқару консолінде ұялы құрылғыларды басқару. Ұялы құрылғыларды басқару мүмкіндігі iOS MDM ұялы құрылғыларын және Android құрылғыларын басқаруға арналған. iOS MDM құрылғылары үшін келесі функциялар бар: • Kaspersky Security Center басқаруындағы құрылғыларды қосу. • Конфигурациялық профильдерді құру және өңдеу, конфигурациялық профильдерді ұялы құрылғыларға орнату. • Ұялы құрылғыларға қолданбаларды App Store® көмегімен, манифест файлдары (.plist) немесе ұялы орнату пакеттері (.ipa) көмегімен орнату. • iOS MDM құрылғыларында пәрмендерді орындау, соның ішінде ұялы құрылғыларды бұғаттау, ұялы құрылғы құпиясөзін қалпына келтіру және ұялы құрылғыдағы барлық деректерді өшіру. Android құрылғылары үшін келесі функциялар бар: • Kaspersky Security Center басқаруындағы құрылғыларды қосу. • Саясат арқылы Kaspersky Endpoint Security for Android басқару. • Құрылғыларда пәрмендерді орындау. Ұялы құрылғыларды басқаруға арналған басқару бірлігі - ұялы құрылғы. Ұялы құрылғы Ұялы құрылғы серверіне қосылғаннан кейін басқарылатын болып саналады.	—	✓ Лицензия кілті Басқару серверінің сипаттарына қосылуы керек.
Kaspersky Security Center Web Console веб-консолінде ұялы құрылғыларды қорғау Kaspersky Security Center Web Console веб-консолі Android және iOS ұялы құрылғыларын басқару үшін келесі мүмкіндіктерді ұсынады: • Kaspersky Security Center басқаруындағы құрылғыларды қосу. • Саясаттарды пайдаланып, Kaspersky Endpoint Security for Android и Kaspersky Security for iOS бағдарламасын басқару. • Тиісті протоколдар мен пәрмендерді орындау арқылы ұялы құрылғыларға пәрмендерді жіберу.	—	✓ Әрбір ұялы құрылғыға лицензия кілті қосылуы керек.
Жүйелерді басқару Келесі функциялар қолжетімді: • Операциялық жүйелер мен бағдарламаларды орнату. Kaspersky Security Center бағдарламасы операциялық жүйелердің кескіндерін орталықтандырылған түрде жасауға және оларды желі арқылы клиент құрылғыларына орналастыруға, сонымен қатар Kaspersky немесе басқа да бағдарламалық жасақтама өндірушілерінің бағдарламаларын қашықтан орнатуға мүмкіндік береді. Сіз құрылғылардың операциялық жүйелерінің кескіндерін қармай алады және бұл кескіндерді Басқару серверіне жеткізе аласыз. Мұндай операциялық жүйелердің кескіндері Басқару серверінде арнайы қалтада сақталады. Эталондық құрылғының операциялық жүйесінің кескінін алу және жасау орнату пакетін жасау тапсырмасы арқылы жүзеге асырылады. Алынған кескіндерді, операциялық жүйе әлі орнатылмаған желідегі жаңа құрылғыларға орналастыру үшін пайдалануға болады. Осы мақсатта Preboot eXecution Environment (PXE) технологиясы қолданылады. • лицензиялы бағдарламалар топтарын басқару; • Microsoft Windows "Қашықтағы жұмыс үстеліне қосылу орындалуда" құрамдасы арқылы клиент құрылғыларына қосылуға қашықтан рұқсат беру. • Windows компьютерлік бөлісу қызметі арқылы клиент құрылғыларына қашықтан қосылу. • **Kaspersky қашықтағы жұмыс үстелі сеансын көру құралы** көмегімен қашықтан қосылу.	—	✓

Функция немесе сипат	Kaspersky Security Center жұмыс режимі	
	Лицензия жоқ	Коммерциялық лицензия
Бұлтты ортамен біріктіру Kaspersky Security Center бағдарламасы физикалық құрылғылармен жұмыс істеп қана қоймайды, сонымен қатар бұлтты ортада жұмыс істеу мүмкіндігін береді, мысалы, бұлттық ортаны конфигурациялау шебері көмегімен. Kaspersky Security Center бағдарламасы келесі виртуалды машиналармен жұмыс істейді: • Amazon EC2 даналары • Microsoft Azure виртуалды машиналары • Google Cloud виртуалды машиналарының даналары • Yandex.Cloud виртуалды машиналары	—	✓
Оқиғаларды SIEM жүйелеріне экспорттау: Syslog протоколы арқылы Syslog протоколы бойынша Kaspersky Security Center Басқару серверінде және басқарылатын құрылғыларды орнатылған Kaspersky бағдарламаларында орын алған кез келген оқиғаларды жіберуге болады. Syslog протоколы – хабарларды тіркеудің стандартты протоколы. Сіз осы протоколды оқиғаларды кез келген SIEM жүйесіне экспорттау үшін қолдана аласыз.	✓	✓

Kaspersky Security Center және басқарылатын бағдарламаларды лицензиялау ерекшеліктері

Басқару сервері мен басқарылатын бағдарламаларды лицензиялаудың келесі ерекшеліктері бар:

- Осалдықтар мен патчтарды басқару, Ұялы құрылғыларды басқару немесе SIEM жүйелерімен біріктіру мүмкіндіктерін белсендіру үшін Басқару серверіне лицензиялық кілтті немесе жарамды белсендіру кодын қосуға болады. Кейбір Kaspersky Security Center функциялары Басқару серверіне қосылған белсенді кілттер немесе жарамды белсендіру кодтары болған кезде ғана қолжетімді.

- Басқару сервер қоймасында басқарылатын бағдарламалар үшін бірнеше белсендіру кодтары мен кілт файлдарын қосуға болады.

Kaspersky Security Center лицензиялау ерекшеліктері

Мысалы, кілт файлы көмегімен мүмкіндіктердің бірін белсендірген болсаңыз (мысалы, Ұялы құрылғыларды басқару), бірақ сізге басқа мүмкіндіктер қажет болса (мысалы, Осалдықтар мен патчтарды басқару), бұл жағдайда екі функционалдықты да іске қосатын кілтті сатып алып, сол кілтпен Басқару серверін іске қосу қажет.

Басқарылатын бағдарламаларды лицензиялау ерекшеліктері

Басқарылатын бағдарламаларды лицензиялау үшін белсендіру кодын немесе кілтті автоматты түрде немесе өзіңізге ыңғайлы басқа жолмен таратуға болады. Белсендіру кодын немесе кілт файлын таратудың келесі жолдары бар:

- Автоматты түрде тарату

Егер сіз әртүрлі басқарылатын бағдарламаларды қолдансаңыз және белгілі бір кілт файлын немесе белсендіру кодын құрылғыларға тарату маңызды болса, белсендіру кодын немесе кілтті таратудың басқа тәсілдерін қолданыңыз.

Kaspersky Security Center қолда бар лицензиялық кілттерді құрылғыларға автоматты түрде таратуға мүмкіндік береді. Мысалы, Басқару сервері қоймасында үш лицензиялық кілт бар. Барлық лицензиялық кілттер үшін **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасы қойылған. Ұйымның құрылғыларында Kaspersky қауіпсіздік бағдарламасы, мысалы, Kaspersky Endpoint Security for Windows орнатылған. Лицензиялық кілтті таратуды қажет ететін жаңа құрылғы табылды. Бағдарлама бұл құрылғыға не сәйкес келетінін анықтайды, мысалы, қоймадан екі лицензиялық кілт, *Кілт_1* лицензиялық кілті және *Кілт_2* лицензиялық кілті. Құрылғыға жарамды лицензиялық кілттердің бірі қолданылады. Бұл жағдайда, осы екі лицензиялық кілттің қайсысы осы құрылғыға қолданылатынын болжау мүмкін емес, өйткені лицензиялық кілттерді автоматты түрде тарату әкімшінің араласуын қамтымайды.

Лицензиялық кілтті құрылғыларға таратқан кезде осы лицензиялық кілт үшін құрылғылар есептеледі. Лицензиялық кілт қолданылатын құрылғылардың саны лицензиялық шектен аспайтынына көз жеткізуіңіз керек. Егер құрылғылардың саны лицензиялық шектен асып кетсе, мұндай құрылғыларға *Критикалық* күйі беріледі.

- Басқарылатын бағдарламаның орнату пакетіне кілт файлын немесе белсендіру кодын қосу.

  Басқарылатын бағдарламаны орнату пакеті арқылы орнатқан жағдайда, белсендіру кодын немесе кілт файлын орнату пакетінде немесе сол бағдарламаның саясатында көрсетуге болады. Лицензиялық кілт, құрылғыны Басқару серверімен кезекті рет синхрондау кезінде басқарылатын құрылғыларға қолданылады.

- Лицензиялы бағдарламалардың лицензиялық кілтін қосу тапсырмасы арқылы тарату

  Басқарылатын қолданбаның лицензия кілтін қосу тапсырмасын пайдалануға тіркелсеңіз, сіз құрылғыларға орнатылатын лицензия кілтін таңдап, құрылғыларды өзіңізге ыңғайлы тәсілмен таңдай аласыз (мысалы, басқару тобын немесе құрылғылар таңдауын таңдау арқылы).

- Құрылғыларға белсендіру кодын немесе кілт файлын қолмен қосу.

Kaspersky бағдарламалары. Орталықтандырылған орналастыру

Бұл бөлімде Kaspersky бағдарламаларын қашықтан орнату және оларды желі құрылғыларынан жою тәсілдері сипатталған.

Клиент құрылғыларына бағдарламаларды орнатуды бастамас бұрын, құрылғылардың аппараттық және бағдарламалық жасақтамасының талаптарға сай екендігіне көз жеткізу қажет.

Басқару серверінің клиент құрылғыларымен байланысын Желілік агент қамтамасыз етеді. Сондықтан, оны қашықтан орталықтандырылған басқару жүйесіне қосылатын әрбір клиент құрылғысына орнату керек. Басқару сервері орнатылған құрылғыда тек Желілік агенттің серверлік нұсқасын пайдалануға болады. Ол Басқару серверінің құрамына кіреді және онымен бірге орнатылып, жойылады. Бұл құрылғыға Желілік агент орнату қажет емес.

Желілік агентті орнату бағдарламаларды орнату сияқты жүзеге асырылады және оны қашықтан да, жергілікті түрде де жасауға болады. Қауіпсіздік бағдарламаларын Басқару консолі арқылы орталықтандырылған түрде орнатқан кезде, сіз Желілік агентті қауіпсіздік бағдарламаларымен бірге орната аласыз.

Желілік агенттер, олар жұмыс істейтін Kaspersky бағдарламаларына байланысты әртүрлі болуы мүмкін. Кейбір жағдайларда тек жергілікті Желілік агентті орнатуға болады (қосымша ақпарат алу үшін тиісті бағдарламаларға арналған Нұсқаулықтарды қараңыз). Клиент құрылғысы Желілік агентті тек бір рет орнату керек.

Басқару консолі арқылы Kaspersky бағдарламаларын басқару жұмысы басқару плагиндерінің көмегімен жүзеге асырылады. Сондықтан, Kaspersky Security Center арқылы бағдарламаны басқаруға қол жеткізу үшін осы бағдарламаны басқару плагині әкімшінің жұмыс станциясына орнатылуы керек.

Бағдарламаларды қашықтан орнатуды әкімші жұмыс станциясынан Kaspersky Security Center бағдарламасының басты терезесінде орындауға болады.

Бағдарламалық жасақтаманы қашықтан орнату үшін қашықтан орнату тапсырмасын жасау керек.

Қалыптасқан қашықтан орнату тапсырмасы оның кестесіне сәйкес іске қосылады. Тапсырманы қолмен орындауды тоқтату арқылы орнату процедурасын тоқтатуға болады.

Қолданбаны қашықтан орнату қатені қайтарса, құрылғыны дайындау талаптарының орындалғанын тексеріңіз.

Орналастыру туралы есеп арқылы желіде Kaspersky қауіпсіздік бағдарламаларын орнату процесін қадағалауға болады.

Kaspersky Security Center арқылы тізімделген бағдарламаларды басқару туралы толық ақпаратты тиісті бағдарламалардың Нұсқаулықтарынан қараңыз.

Үшінші тарап қауіпсіздік бағдарламаларын алмастыру

Kaspersky қауіпсіздік бағдарламаларын Kaspersky Security Center құралдарымен орнату үшін, орнатылатын бағдарламамен үйлеспейтін үшінші тарап бағдарламалық жасақтамасын жою қажет болуы мүмкін. Kaspersky Security Center, үшінші тарап бағдарламаларын жоюдың бірнеше тәсілін ұсынады.

Үйлесімсіз бағдарламаларды орнату бағдарламасы арқылы жою

Бұл параметр тек Microsoft Management Console басқару консолі негізіндегі Басқару консолінде қолжетімді.

Үйлесімді емес бағдарламалар жою әдісін әртүрлі орнату түрлері қолдайды. Қауіпсіздік бағдарламасын орнатпас бұрын, егер қауіпсіздік бағдарламасының орнату пакетінің сипаттары терезесінде (**Үйлесімді емес бағдарламалар** бөлімі) **Үйлесімді емес бағдарламаларды автоматты түрде жою** параметрі таңдалса, онымен үйлеспейтін бағдарламалар автоматты түрде жойылады.

Бағдарламаны қашықтан орнатуды кезінде үйлесімсіз бағдарламаларды жою

Қауіпсіздік бағдарламасын қашықтан орнату кезінде **Үйлесімді емес бағдарламаларды автоматты түрде жою** параметрін қосуға болады. Microsoft Management Console (MMC) консолі негізіндегі Басқару консолінде, бұл параметр қашықтан орнату шеберінде қолжетімді. Kaspersky Security Center Web Console бағдарламасында, бұл параметрді қорғанысты орналастыру шеберінде табуға болады Егер бұл параметр қосулы болса, Kaspersky Security Center бағдарламасы басқарылатын құрылғыға қауіпсіздік бағдарламасын орнатпас бұрын, үйлесімсіз бағдарламаларды жояды.

Нұсқаулар:

- Басқару консолі: үйлесімді емес бағдарламаларды қашықтан орнату шебері арқылы жою.
- Kaspersky Security Center Web Console: Орнатудың алдында үйлесімді емес бағдарламаларды жою.

Үйлесімсіз бағдарламаларды бөлек тапсырма арқылы жою

Үйлесімсіз бағдарламаларды жою үшін **Бағдарламаны қашықтан жою** тапсырмасы қолданылады. Тапсырма қауіпсіздік бағдарламасын орнату тапсырмасынан бұрын, құрылғыларда іске қосылуы керек. Мысалы, орнату тапсырмасында **Басқа тапсырманы аяқтағанда** түрі кестесін таңдауға болады, мұндағы басқа тапсырма – **Бағдарламаны қашықтан жою** тапсырмасы болып табылады.

Бұл жою тәсілі, қауіпсіздік бағдарламасы инсталляторы үйлесімсіз бағдарламалардың ешқайсысын сәтті жоя алмаған жағдайда қолданылғаны жөн.

Басқару консоліне арналған нұсқаулар: Жаңа тапсырма қосу.

Қашықтан орнату тапсырмасын пайдаланып бағдарламаларды орнату

Kaspersky Security Center қашықтан орнату тапсырмаларын пайдаланып құрылғыларға бағдарламаларды қашықтан орнатуға мүмкіндік береді. Тапсырмалар шебердің көмегімен жасалады және құрылғыларға тағайындалады. Құрылғыларға (ең көбі 1000 құрылғы) тапсырманы тезірек және оңай тағайындау үшін құрылғы шебері терезесінде өзіңізге ыңғайлы түрде көрсете аласыз:

- **Басқару серверімен анықталған желілік құрылғыларды таңдау**. Құрылғылар жинағына тапсырма тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.
- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**. Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.
- **Құрылғы таңдауына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған таңдауды құрайтын құрылғыларға тағайындалады. Алдын ала анықталған таңдауды немесе өз таңдауыңызды көрсете аласыз.
- **Басқару тобына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады.

Қолданбаны желілік агент орнатылмаған клиент құрылғысына орнату кезінде туындауы мүмкін мәселелерге жол бермеу үшін Kaspersky Security Center қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру процедурасында сипатталғандай әрекет ету керек.

Бағдарламаны таңдалған құрылғыларға орнату

Қолданбаны таңдалған құрылғыларға орнату үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Тапсырма жасау** түймесі бойынша тапсырманы жасау шеберін іске қосыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде, **Kaspersky Security Center Басқару сервері** түйінінде **Бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.

   Жаңа тапсырма жасау шебері жұмысының нәтижесінде таңдалған құрылғылар жиынтығы үшін таңдалған бағдарламаны қашықтан орнату тапсырмасы жасалады. Жасалған тапсырма **Тапсырмалар** қалтасының жұмыс аймағында көрсетіледі.
3. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындау нәтижесінде таңдалған бағдарлама таңдалған құрылғыларға орнатылады.

Бағдарламаны басқару тобының клиент құрылғыларына орнату

Бағдарламаны басқару тобының клиент құрылғыларына орнату үшін:

1. Қажетті басқару тобын басқаратын Басқару серверіне қосылыңыз.
2. Консоль ағашында басқару топтарын таңдаңыз.
3. Жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.
4. **Тапсырма жасау** түймесі бойынша тапсырманы жасау шеберін іске қосыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде, **Kaspersky Security Center Басқару сервері** түйінінде **Бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.

   Жаңа тапсырма жасау шеберінің жұмысы нәтижесінде, таңдалған бағдарламаны қашықтан орнатудың топтық тапсырмасы жасалады. Жасалған тапсырма басқару тобының жұмыс аймағында, **Тапсырмалар** қойыншасында көрсетіледі.
5. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындау нәтижесінде таңдалған бағдарлама басқару тобының клиент құрылғыларына орнатылады.

Active Directory топтық саясаты арқылы бағдарламаны орнату

Kaspersky Security Center бағдарламасы Active Directory топтық саясаттарының көмегімен басқарылатын құрылғыларға Kaspersky бағдарламаларын орнатуға мүмкіндік береді. Басқару сервер құрылғысы басқарылатын құрылғылармен бір доменде болуы керек.

Active Directory топтық саясаттарының көмегімен бағдарламаларды орнату тек Желілік агент кіретін орнату пакеттерінен ғана мүмкін болады.

Бағдарламаны Active Directory топтық саясаттары көмегімен орнату үшін:

1. Бағдарламаны орнату конфигурациясын қашықтан орнату шебері көмегімен бастаңыз.
2. Қашықтан орнату шеберінің **Қашықтан орнату тапсырмасының параметрлерін анықтау** терезесінде **Active Directory топтық саясаттарында бума орнатуды тағайындау** параметрін таңдаңыз.
3. Қашықтан орнату шеберінің **Құрылғыларға қатынасу үшін есептік жазбаларды таңдау** терезесінде **Есептік жазба қажет (Желілік агент пайдаланылмайды)** параметрін таңдаңыз.
4. Kaspersky Security Center бағдарламасы орнатылған құрылғыға немесе Иеленушілер-топтық саясатты жасаушылар домендік тобына кіретін есептік жазбаға әкімші құқықтары бар есептік жазбаны қосыңыз.
5. Таңдалған есептік жазбаға рұқсаттар беріңіз:
   a. **Басқару тақтасы** → **Басқару** тармағына өтіңіз және **Топтық саясатты басқару** тармағын ашыңыз.
   b. Қажетті домені бар түйінді басыңыз.
   c. **Табыстау** бөлімін басыңыз.
   d. **Қатынасу құқықтары** ашылмалы тізімінде **GPO байланыстырылған нысандары** тармағын таңдаңыз.
   e. **Қосу** түймесін басыңыз.
   f. Ашылған **Пайдаланушыны, компьютерді немесе топты таңдау** терезесінде қажетті есептік жазбаны таңдаңыз.
   g. **Пайдаланушыны, компьютерді немесе топты таңдау** терезесін жабу үшін **OK** түймесін басыңыз.
   h. **Топтар және пайдаланушылар** тізімінде жаңа ғана қосылған есептік жазбаны таңдаңыз және **Қосымша** → **Қосымша** түймесін басыңыз.
   i. **Рұқсаттар жазбалары** тізімінде жаңа ғана қосылған есептік жазбаны екі рет басыңыз.
   j. Келесі рұқсаттар беріңіз:
      - **топ нысандарын жасау;**
      - **топ нысандарын жою;**

- **топтық саясат контейнерінің нысандарын жасау;**
- **топтық саясат контейнерінің нысандарын жою.**

k. Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

6. Шебердің нұсқауларын орындай отырып, басқа параметрлерді белгілеңіз.
7. Жасалған қашықтан орнату тапсырмасын қолмен іске қосыңыз немесе оның кесте бойынша іске қосылуын күтіңіз.

Нәтижесінде, келесі қашықтан орнату механизмі іске қосылады:

1. Тапсырманы іске қосқаннан кейін, жиынтықтағы клиент құрылғылары тиесілі болып табылатын әр доменде келесі нысандар жасалады:
   - **Kaspersky_AK{GUID}** атты топтық саясат нысаны (Group policy object, GPO).
   - Қауіпсіздік тобында тапсырма таратылатын клиент құрылғылары бар. Бұл қауіпсіздік тобында тапсырма таратылатын клиент құрылғылары бар. Қауіпсіздік тобының құрамы топтық саясат нысаны (GPO) аймағын анықтайды.
2. Kaspersky Security Center таңдалған Kaspersky қолданбаларын клиент құрылғыларына тікелей KLSHARE арқылы, яғни қолданбаның желілік ортақ қатынасы бар қалтасынан орнатады. Бұл ретте, Kaspersky Security Center орнату қалтасында орнатылып жатқан бағдарлама үшін msi кеңейтімі бар файлды қамтитын салынған қосалқы қалта жасалады.
3. Тапсырманың әрекет ету ауқымына жаңа құрылғылар қосылған кезде, олар келесі тапсырманы іске қосқаннан кейін қауіпсіздік тобына қосылады. Егер тапсырманың кестесінде **Өткізіп алынған тапсырмаларды іске қосу** жалаушасы таңдалған болса, құрылғылар қауіпсіздік тобына бірден қосылады.
4. Құрылғыларды тапсырманың әрекет ету аумағынан алып тастаған кезде, оларды қауіпсіздік тобынан жою келесі тапсырманы іске қосқан кезде орын алады.
5. Тапсырманы Active Directory-ден жойған кезде топтық саясат нысаны (GPO), топтық саясат нысанына (GPO) келтірілген сілтеме және тапсырмамен байланысты қауіпсіздік тобы жойылады.

Егер сіз Active Directory арқылы басқа орнату схемасын қолданғыңыз келсе, орнату параметрлерін қолмен конфигурациялай аласыз. Бұл, мысалы, келесі жағдайларда қажет болуы мүмкін:

- әкімшіде кейбір домендердің Active Directory қызметіне өзгерістер енгізу құқығының антивирустық қорғанысы болмаған жағдайда;
- егер бастапқы дистрибутивті бөлек желілік ресурста орналастыру қажет болса;
- топтық саясатты Active Directory қызметінің нақты бөлімшелеріне байланыстыру.

Active Directory арқылы басқа орнату схемасын пайдаланудың келесі нұсқалары бар:

- Егер тікелей Kaspersky Security Center ортақ қатынасы бар қалтасынан орнату қажет болса, Active Directory топтық саясатының сипаттарында қажетті бағдарламаның орнату пакетінің қалтасына салынған exec қалтасында орналасқан msi кеңейтімі бар файлды көрсету керек.
- Егер орнату пакетін басқа желілік ресурсқа орналастыру қажет болса, оған exec қалтасының барлық мазмұнын көшіріп алу керек, өйткені MSI кеңейтімі бар файлдан басқа, ол орнату пакетін жасау кезінде қалыптасқан конфигурация файлдарын да қамтиды. Лицензиялық кілтті бағдарламамен бірге орнату үшін кілт файлын осы қалтаға көшіріп алу керек.

Қолданбаларды macOS құрылғыларына қашықтан орнату

Қашықтан орнату тапсырмасын пайдаланып, macOS жүйесі бар құрылғыларға қолданбаларды орнату үшін:

1. Орнату пакеті мен .sh орнату сценарийінен тұратын мұрағат жасаңыз.

2. Жаңа тапсырма шеберіндегі **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру** опциясын өшіріңіз.

Болмаса **Сценарийлерді қашықтан іске қосу** тапсырмасын пайдалануға болады. Келесі мақалада осы тапсырма үшін файлдарды конфигурациялау жолы сипатталған: Скриптілерді қашықтан орындау тапсырмасын пайдаланып, құрылғыларға қолданбаларды қашықтан орнату.

Қосалқы Басқару серверлеріне бағдарламаларды орнату

Бағдарламаны қосалқы Басқару серверлеріне орнату үшін:

1. Өзіңізге қажетті қосалқы Басқару серверлерін басқаратын Басқару серверіне қосылыңыз.

2. Орнатылған бағдарламаға сәйкес орнату пакеті таңдалған қосалқы Басқару серверлерінің әрқайсысында екеніне көз жеткізіңіз. Егер орнату пакеті қандай да бір қосалқы Серверлерде болмаса, оны орнату пакетін тарату тапсырмасы арқылы таратыңыз.

3. Келесі тәсілдердің бірімен бағдарламаны қосалқы Басқару серверлеріне орнату тапсырмасын құруды бастаңыз:

   - Егер сіз таңдалған басқару тобының қосалқы Серверлері үшін тапсырма жасағыңыз келсе, сол топ үшін қашықтан орнату топтық тапсырмасын жасауды бастаңыз.

   - Егер сіз қосалқы Серверлер жиынтығы үшін тапсырма жасағыңыз келсе, құрылғылар жиынтығы үшін қашықтан орнату тапсырмасын жасауды бастаңыз.

   Нәтижесінде, қашықтан орнату тапсырмаларын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде, **Kaspersky Security Center Басқару сервері** түйінінде, **Кеңейтілген** қалтасында **Қосалқы Басқару серверіне бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.

   Жаңа тапсырма шебері таңдалған қолданбаны нақты қосымша басқару серверлеріне қашықтан орнату тапсырмасын жасайды.

4. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындау нәтижесінде таңдалған бағдарлама таңдалған қосалқы Басқару серверлеріне орнатылады.

Қашықтан орнату шеберін пайдаланып бағдарламаларды орнату

Kaspersky бағдарламаларын орнату үшін қашықтан орнату шеберін пайдалануға болады. Қашықтан орнату шебері, қалыптасқан орнату пакеттерін де, дистрибутивтерді де қолдана отырып, бағдарламаларды қашықтан орнатуға мүмкіндік береді.

Қашықтан орнату тапсырмасы Желілік агент орнатылмаған клиент құрылғысында дұрыс жұмыс істеуі үшін TCP 139 және 445, UDP 137 және 138 порттарын ашу қажет. Бұл порттар әдепкі бойынша доменге қосылған барлық құрылғыларда ашық. Желі қателері болған жағдайда, Kaspersky Security Center білім қорын қараңыз.

Бағдарламаны таңдалған құрылғыларға қашықтан орнату шебері арқылы орнату үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында орнатылатын бағдарламаның орнату пакетін таңдаңыз.
3. Орнату пакетінің мәнмәтіндік мәзірінде **Бағдарламаны орнату** тармағын таңдаңыз.

   Қашықтан орнату шебері іске қосылады.
4. **Орнату үшін құрылғыларды таңдау** терезесінде бағдарлама орнатылатын құрылғылардың тізімін жасауға болады:

   - **Басқарылатын құрылғылар тобына орнату**

     Егер бұл нұсқа таңдалса, құрылғылар тобы үшін бағдарламаны қашықтан орнату тапсырмасы жасалады.

   - **Орнату үшін құрылғыларды таңдау**

     Егер бұл нұсқа таңдалса, құрылғылар жиынтығы үшін бағдарламаны қашықтан орнату тапсырмасы жасалады. Жиынтықтың құрамына топтардың құрамындағы құрылғылар да, тағайындалмаған құрылғылар да кіруі мүмкін.
5. **Қашықтан орнату тапсырмасының параметрлерін анықтау** терезесінде бағдарламаны қашықтан орнату параметрлерін конфигурациялаңыз.

   Орнату пакетін мәжбүрлеп жүктеп алу параметрлер блогында бағдарламаны орнату үшін қажетті файлдарды клиент құрылғыларына жеткізу тәсілін таңдаңыз:

   - **Желілік агенттің көмегімен**

     Егер бұл параметр қосылса, орнату пакеттерін клиент құрылғыларына жеткізуді клиент құрылғыларына орнатылған Желілік агент жүзеге асырады.

     Егер бұл параметр өшірулі болса, орнату пакеттері клиент құрылғысының операциялық жүйесі құралдарының көмегімен жеткізіледі.

     Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

     Әдепкі бойынша, параметр қосулы.

- **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

  Бұл параметр қосылса, файлдар Басқару сервері көмегімен клиент құрылғыларының операциялық жүйесі арқылы клиент құрылғыларына жеткізіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

  Әдепкі бойынша, параметр қосулы.

- **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

  Егер бұл параметр қосылса, орнату пакеттері тарату нүктелері арқылы операциялық жүйенің көмегімен клиент құрылғыларына беріледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл нұсқаны таңдауға болады.

  Желілік агент көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

  Әдепкі бойынша, параметр виртуалды Басқару серверінде жасалған қашықтан орнату тапсырмалары үшін қосылған.

  > Құрылғыға тағайындалған барлық тарату нүктелері ақаулы болған кезде, құрылғы жаңартуларды (антивирустық дерекқорлар мен патчтарды) және орнату пакеттерін алмайды.

- **Орнату әрекеттерінің саны**

  Kaspersky Security Center қашықтан орнату тапсырмасын іске қосу кезінде параметрлерде көрсетілген орнатуды іске қосу саны ішінде басқарылатын құрылғыға бағдарламаны орнату мүмкін болмаса, Kaspersky Security Center бағдарламасы осы басқарылатын құрылғыға орнату пакетін жеткізуді тоқтатады және бұдан былай құрылғыда орнатуды іске қоспайды.

  `Орнату әрекеттерінің саны` параметрі басқарылатын құрылғы ресурстарын сақтауға, сондай-ақ трафикті азайтуға мүмкіндік береді (жою, MSI файлын іске қосу және қате туралы хабарлар).

  Тапсырманы бірнеше рет іске қосу әрекеттері орнатуға кедергі келтіретін құрылғыдағы ақаулықты көрсетуі мүмкін. Әкімші орнату әрекеттерінің көрсетілген саны ішінде мәселені шешуі (мысалы, дискіде жеткілікті орын бөлу, үйлесімсіз бағдарламаларды жою немесе орнатуға кедергі келтіретін басқа бағдарламалардың параметрлерін өзгерту арқылы) және тапсырманы қайта іске қосуы (қолмен немесе кесте бойынша) керек.

  Егер орнату орындалмаса, мәселе шешілмейтін болып саналады және кез келген кейінгі іске қосу әрекеттері ресурстар мен трафиктің қажетсіз шығыны тұрғысынан қымбат болып саналады.

  Тапсырма жасалғаннан кейін, орнату әрекеттерінің саны `0`-ге тең болады. Құрылғыдағы қатені қайтаратын әрбір орнатуды іске қосу есептегіштің көрсеткіштерін арттырады.

  Егер тапсырма параметрлерінде көрсетілген орнату әрекеттерінің саны асып кетсе және құрылғы бағдарламаны орнатуға дайын болса, сіз `Орнату әрекеттерінің саны` параметрінің мәнін арттырып, бағдарламаны орнату тапсырмасын орындай аласыз. Сондай-ақ, сіз қашықтан орнату тапсырмасының басқасын жасай аласыз.

Басқа Басқару сервері басқаратын клиент құрылғыларымен қандай әрекетті орындау керектігін анықтаңыз:

- **Барлық құрылғыларда орнату**

  Бағдарлама тіпті басқа Басқару серверлері басқаратын құрылғыларға орнатылады.

  Әдепкі бойынша, осы нұсқа таңдалады. Желіде тек бір Басқару сервері болса, бұл параметрді өзгертудің қажеті жоқ.

- **Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату**

  Бағдарлама тек осы Басқару сервері басқаратын құрылғыларға орнатылады. Егер сіздің желіңізде бірнеше Басқару сервері орнатылған болса және олардың арасындағы қайшылықтардан аулақ болғыңыз келсе, осы параметрді таңдаңыз.

Қосымша параметрлерді конфигурациялаңыз:

- **Бұрын орнатылып қойған жағдайда, бағдарламаны қайта орнатпау**

  Егер бұл параметр қосылса, таңдалған бағдарлама клиент құрылғысында орнатылған болса, қайта орнатылмайды.

  Егер бұл параметр өшірулі болса, бағдарлама кез келген жағдайда орнатылады.

  Әдепкі бойынша, параметр қосулы.

- **Active Directory топтық саясаттарында бума орнатуды тағайындау**

  Егер бұл параметр қосылса, орнату пакеті Active Directory топтық саясаттары арқылы орнатылады.

  Егер Желілік агенттің орнату пакеті таңдалса, параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

6. **Лицензия кілтін таңдау** терезесінде лицензиялық кілтті және оны қалай тарату керектігін таңдаңыз:

   - **Лицензиялық кілтті орнату пакетіне орналастырмау (ұсынылады)**

     Егер бұл нұсқа таңдалса, кілт автоматты түрде сәйкес келетін құрылғыларға таратылады:

     - егер кілттің сипаттарында автоматты түрде тарату конфигурацияланған болса;
     - **Кілтті қосу** тапсырмасы жасалған болса.

   - **Лицензиялық кілтті орнату пакетіне орналастыру**

     Кілт орнату пакетімен бірге құрылғыларға таралады.

     > Кілтті осылайша тарату ұсынылмайды, өйткені әдепкі бойынша орнату пакетінің қоймасы оқуға ортақ қатынасуға конфигурацияланған.

   Лицензия кілтін таңдау терезесі, орнату пакетінде лицензиялық кілт болмаса көрсетіледі.

   Егер орнату пакеті лицензиялық кілтті қамтыса, лицензиялық кілт туралы ақпараты бар **Лицензиялық кілттің сипаттары** терезесі көрсетіледі.

7. **Операциялық жүйені қайта іске қосу параметрін таңдау** терезесінде бағдарламаларды орнату барысында операциялық жүйені қайта іске қосу қажет болса, құрылғыларды қайта іске қосуды анықтаңыз:

   - **Құрылғыны қайта іске қоспау**

     Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылмайды.

   - **Құрылғыны қайта іске қосу**

     Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылады.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Егер бұл нұсқа таңдалса, қауіпсіздік бағдарламасын орнатқаннан кейін пайдаланушыға құрылғыны қайта іске қосу туралы хабар көрсетіледі. **Өзгерту** сілтемесінде хабар мәтінін, сондай-ақ хабардың көрсетілу мерзімін және автоматты түрде қайта іске қосу уақытын өзгертуге болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Бұл опция таңдалса, бұғатталған құрылғылардағы қолданбалар қайта бастау алдында мәжбүрлі түрде жабылады.

  Әдепкі бойынша, параметр өшірулі.

8. **Құрылғыларға қатынасу үшін есептік жазбаларды таңдау** терезесінде қашықтан орнату тапсырмасын іске қосу үшін пайдаланылатын есептік жазбаларды қосуға болады:

   - **Есептік жазба қажет емес (Желілік агент орнатылды)**

     Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

     Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

   - **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

     Егер сіз қашықтан орнату тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда бағдарламаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

     - **Жергілікті есептік жазба**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті есептік жазба** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

       Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

     - **SSH сертификаты**. Бағдарламаны Linux басқаратын клиенттік құрылғыға орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

       Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Назар аударыңыз, Kaspersky Security Center, PEM жабық кілттері пішімін қолдайды, бірақ ssh-keygen утилитасы әдепкі бойынша OPENSSH пішіміндегі SSH кілттерін генерациялайды. OPENSSH пішімін Kaspersky Security Center қолдайды. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз. Мысалы:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "< пайдаланушының электрондық поштасы >"
       ```

9. **Орнатуды бастау** терезесінде, таңдалған құрылғыларда қашықтан орнату тапсырмасын жасау және іске қосу үшін **Келесі** түймесін басыңыз.

   Орнатуды бастау терезесінде **Қашықтан орнату шеберінің жұмысы аяқталғаннан кейін тапсырманы іске қоспау** параметрі таңдалған болса, қашықтан орнату тапсырмасы іске қосылмайды. Бұл тапсырманы кейінірек қолмен іске қосуға болады. Тапсырма атауы бағдарламаны орнатуға арналған орнату пакетінің атауына сай келеді: **<Орнату пакетінің атауы> орнату**.

Бағдарламаны басқару тобының құрылғыларына қашықтан орнату шебері арқылы орнату үшін:

1. Қажетті басқару тобын басқаратын Басқару серверіне қосылыңыз.
2. Консоль ағашында басқару топтарын таңдаңыз.
3. Топтың жұмыс аймағында **Әрекетті орындау** түймесін басып, ашылмалы тізімнен **Бағдарламаны орнату** тармағын таңдаңыз.

   Нәтижесінде, қашықтан орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
4. Шебердің соңғы қадамында, таңдалған құрылғыларда қашықтан орнату тапсырмасын жасау және іске қосу үшін **Келесі** түймесін басыңыз.

Қашықтан орнату шебері аяқталғаннан кейін, Kaspersky Security Center бағдарламасы келесі әрекеттерді орындайды:

- Бағдарламаны орнату үшін орнату пакетін жасайды (егер ол бұрын жасалмаған болса). Орнату пакеті **Қашықтан орнату** қалтасында, бағдарламаның атауы мен нұсқасына сай келетін атауы бар **Орнату пакеттері** салынған қалтада орналастырылады. Бағдарламаны кейінірек орнату үшін осы орнату пакетін пайдалануға болады.
- Құрылғылар жиынтығы немесе басқару тобы үшін қашықтан орнату тапсырмасын жасайды және іске қосады. Қалыптасқан қашықтан орнату тапсырмасы **Тапсырмалар** қалтасына орналастырылады немесе ол құрылған басқару тобының тапсырмаларына қосылады. Бұл тапсырманы кейінірек қолмен іске қосуға болады. Тапсырма атауы бағдарламаны орнатуға арналған орнату пакетінің атауына сай келеді: **<Орнату пакетінің атауы> орнату**.

Басқару плагиндерімен жұмыс істеу

Басқару консолі арқылы Kaspersky бағдарламаларын басқару жұмысы басқару плагиндерінің көмегімен жүзеге асырылады. Kaspersky Security Center көмегімен басқаруға болатын әрбір Kaspersky бағдарламасының құрамына басқару плагині кіреді. Басқару консолиндегі бағдарламаны басқару плагинінің көмегімен келесі әрекеттерді орындауға болады:

- бағдарламалар мен олардың параметрлерінің, сондай-ақ бағдарламаларға арналған параметрлердің саясаттарын жасау және өзгерту;
- бағдарламаның тапсырмалары, оның жұмысындағы оқиғалар, сондай-ақ клиент құрылғыларынан алынған бағдарламалардың жұмыс статистикасы туралы ақпарат алу.

Орнатылған плагиндер тізімін және олардың нұсқаларын тексеру үшін:

1. Басқару консолінің тармақты құрылымында **<Сервер атауы> басқару серверін** тінтуірдің оң жақ түймесімен басып, **Сипаттар** опциясын таңдаңыз.
2. **Кеңейтілген** → **Орнатылған бағдарламаны басқару плагиндерінің мәліметтері** тармағын таңдаңыз.

Орнатылған басқару плагиндерінің тізімдері және олардың нұсқалары оң жақ тақтада пайда болады.

Kaspersky Security Center бастапқы орнату кезінде басқару серверінің жылдам іске қосу шеберін қосқан жағдайда басқарылатын құрылғыларға арналған плагиндерді орнатуға болады. Басқару плагиндерін қолмен орнатуға да болады.

Басқару плагинін қолмен орнату үшін:

1. Kaspersky техникалық қолдау қызметінің бетінен Kaspersky бағдарламасын басқару плагинін және бағдарламаның қажетті нұсқасын (мысалы, Kaspersky Endpoint Security for Windows 12.6) жүктеп алыңыз.

2. Басқару консолі іске қосылған болса, оны жабыңыз.

3. Плагиннің жүктеп алынған файлын мұрағаттан шығарып, klcfginst.msi немесе klcfginst.exe файлын іске қосыңыз. Орнату шеберінің нұсқауларын орындаңыз.

4. Орнату аяқталғаннан кейін, басқару консолін іске қосып, алдыңғы процедурада сипатталғандай, плагиннің орнатылған плагиндер тізімінде бар екеніне көз жеткізіңіз.

Басқарылатын бағдарламаларды бастапқы орнату шеберін қолдайтын басқару плагинін орнатқаннан кейін, басқару консолін іске қосқан кезде бұл шебер автоматты түрде іске қосылады. Kaspersky бағдарламалары үшін әдепкі саясаттар мен тапсырмаларды жасау үшін Басқарылатын қолданбаларды бастапқы орнату шеберінің қадамдарын орындауға болады. Плагинді бастапқы орнатқаннан кейін немесе басқару плагинін тапсырмалары мен саясаты әлі жасалмаған Kaspersky бағдарламасының басқа нұсқасымен үйлесімді нұсқаға жаңартқаннан кейін ғана Басқару консолін іске қосқанда шебер автоматты түрде іске қосылады. Басқарылатын бағдарламалардың бастапқы орнату шеберін қолмен де іске қосуға болады.

Басқарылатын бағдарламаларды бастапқы орнату шеберін іске қосу үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.

2. Басқару сервері түйінінің контекстік мәзірінде **Барлық тапсырмалар → Басқарылатын бағдарламаны жылдам іске қосу шебері** тармағын таңдаңыз.

3. Басқарылатын қолданбаларды бастапқы орнату шебері іске қосылады. Әдепкі параметрлері бар Kaspersky бағдарламаларының саясаттары мен тапсырмаларын жасау үшін шебердің нұсқауларын орындаңыз.

Басқару плагинін жою үшін:

1. Басқару консолі іске қосылған болса, оны жабыңыз.

2. Windows операциялық жүйесінің тізілім редакторын ашыңыз.

3. Келесі кілтті табыңыз:

   - 32 разрядтық жүйе үшін `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins`.
   - 64 разрядтық жүйе үшін `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins`.

   Кілтте орнатылған басқару плагиндері бар. Әрбір плагин үшін `DisplayName` мәні плагин атауын, ал `UninstallString` мәні плагинді жою пәрменін қамтиды.

4. Жойғыңыз келетін плагин кілтін тауып, оның `UninstallString` мәнін алмасу буферіне көшіріңіз.

5. Мәнді пәрмен жолына қойып, оны жүйелік әкімші ретінде іске қосыңыз.

Басқару плагинінің нұсқасы басқарылатын Kaspersky қолданбасының нұсқасынан төмен болмауы керек. Kaspersky қолданбасын жаңарту кезінде құрылғыларға сол нұсқадағы басқару плагинін орнату керек.

Плагиннің бұрынғы нұсқасында жасалған саясатты ашқан кезде, сізден Kaspersky Security Network мәлімдемесін қабылдау сұралады.

Kaspersky Security Center Web Console веб-консолін жойған кезде, барлық басқару плагиндері де жойылады.

Саясатты басқарылатын бағдарлама нұсқасынан кейінгі плагин нұсқасында ашып, сақтасаңыз, саясат жаңартылады және оны плагиннің бұрынғы нұсқасында аша алмайсыз.

Қорғаныс орналастыру туралы есепті қарап шығу

Желіде қорғанысты орналастыру процесін қадағалау үшін қорғаныс орналастыру туралы есепті қолдануға болады.

Қорғаныс орналастыру туралы есепті қарап шығу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.

2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.

3. **Есептер** қойыншасының жұмыс аймағында **Қорғанысты орналастыру туралы есеп** есебінің шаблонын таңдаңыз.

Жұмыс аймағында қорғанысты желінің барлық құрылғыларында орналастыру туралы ақпаратты қамтитын есеп қалыптастырылады.

Қорғаныс орналастыру туралы есептің жаңасын құрастыра аласыз және оған қандай түрдегі ақпаратты қосу керектігін көрсете аласыз:

- басқару тобы үшін;
- арнайы құрылғылар үшін;
- құрылғыны таңдау үшін;
- барлық құрылғылар үшін.

Kaspersky Security Center шеңберінде, құрылғыда қауіпсіздік бағдарламасы орнатылған және нақты уақыт режимінде қорғаныс қосылған жағдайда қорғаныс орналастырылған деп есептеледі.

Бағдарламаларды қашықтан жою

Kaspersky Security Center қашықтан жою тапсырмаларын пайдаланып құрылғылардан бағдарламаларды қашықтан жоюға мүмкіндік береді. Тапсырмалар шебердің көмегімен жасалады және құрылғыларға тағайындалады. Құрылғыларға тапсырманы тезірек және оңай тағайындау үшін құрылғы шебері терезесінде өзіңізге ыңғайлы түрде көрсете аласыз:

- **Басқару серверімен анықталған желілік құрылғыларды таңдау**. Құрылғылар жинағына тапсырма тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**. Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған таңдауды құрайтын құрылғыларға тағайындалады. Алдын ала анықталған таңдауды немесе өз таңдауыңызды көрсете аласыз.

- **Басқару тобына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады.

Қашықтан өшіру мәселелері

Үшінші тарап қолданбаларын қашықтан өшірген кезде, әкімшілерге "Қашықтан өшіру осы құрылғыда ескертулермен аяқталды: өшірілетін қолданба орнатылмаған" деген ескерту көрсетілуі мүмкін. Бұл мәселе әдетте өшірілетін қолданба тек қазір жүйеге кірген жеке пайдаланушы үшін орнатылған кезде туындайды. Пайдаланушы жүйеге кірмеген болса, мұндай қолданба көрінбейтін болады және оны қашықтан өшіруге бағыттау мүмкін емес.

Бұл әрекет бір құрылғыда бірнеше пайдаланушының қолданысына арналған қолданбалардан өзгеше, бұл жағдайда қолданбалар жаһандық деңгейде көрінеді және оларға құрылғының барлық пайдаланушысы қол жеткізе алады.

Kaspersky Security Center ішінде қолданбаларды тіркеу алгоритмі жеке пайдаланушыларға арналған қолданбаларды және бірнеше пайдаланушыға арналған қолданбаларды басқаша өңдейді:

- Бірнеше пайдаланушыға арналған қолданбалар орнатылған қолданбалардың нақты уақыттағы жаңартылған тізімінде сақталады.

- Жеке пайдаланушыларға арналған қолданбалар кэштеу механизмі арқылы бақыланады.

  Пайдаланушы қолданбаны анықтау кезінде жүйеге кірген болса, Kaspersky Security Center сол пайдаланушы қолданбалары туралы ақпаратты кэштейді. Пайдаланушы кейін жүйеден шықса да, Kaspersky Security Center бұл қолданбаларды кэштелген деректер негізінде орнатылған ретінде көрсетуді жалғастырады, бірақ олар құрылғыда енді көрінбейді немесе қолжетімді болмайды.

Бұл сәйкессіздік Kaspersky Security Center кэштелген деректер негізінде орнатылған қолданбаны анықтайтын жағдайларға әкелуі мүмкін, бірақ қолданбаны өшіру тапсырмасы сәтсіз аяқталады, себебі пайдаланушы жүйеден шыққан кезде, қолданбаға қол жеткізу мүмкін емес.

Әдепкі бойынша кэштелген қолданба деректерінің қызмет ету мерзімі 30 күнге орнатылады. Әкімшілер бұл параметрді кэш ұзақтығын қысқарту үшін өзгерте алады, осылайша көрсетілген деректер мен құрылғылардағы қолданбаның нақты көрінуі арасындағы сәйкессіздіктер азаяды.

Кэштің қызмет ету мерзімін 1 сағатқа (3600 секундқа) реттеу үшін басқару серверінде келесі пәрменді іске қосыңыз:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Осы пәрменді іске қосқаннан кейін, өзгерістер күшіне енуі үшін, басқару серверін қайта іске қосыңыз.

Орнатылған қолданбалар туралы ақпарат көзі

Желілік агент Windows құрылғыларына орнатылған бағдарламалық жасақтама туралы ақпаратты келесі тіркеу кілттерінен алады:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Барлық пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  Барлық пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Ағымдағы пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Нақты пайдаланушылар үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

Басқару тобының клиент құрылғыларынан бағдарламаны қашықтан жою

Басқару тобының клиент құрылғыларынан бағдарламаны қашықтан жою үшін:

1. Қажетті басқару тобын басқаратын Басқару серверіне қосылыңыз.
2. Консоль ағашында басқару топтарын таңдаңыз.
3. Жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.
4. **Жаңа тапсырма** түймесі бойынша тапсырманы жасау шеберін іске қосыңыз.
   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
   Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде, **Kaspersky Security Center Басқару сервері** түйінінде, **Кеңейтілген Бағдарламаны қашықтан жою** тапсырма түрін таңдаңыз.

Жаңа тапсырма жасау шеберінің жұмысы нәтижесінде, таңдалған бағдарламаны қашықтан жоюдың топтық тапсырмасы жасалады. Жасалған тапсырма басқару тобының жұмыс аймағында, **Тапсырмалар** қойыншасында көрсетіледі.

5. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан жою тапсырмасын орындау нәтижесінде таңдалған бағдарлама басқару тобының клиент құрылғыларынан жойылады.

Таңдалған құрылғылардан бағдарламаны қашықтан жою

Таңдалған құрылғылардан бағдарламаны қашықтан жою үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. **Жаңа тапсырма** түймесі бойынша тапсырманы жасау процесін іске қосыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде, **Kaspersky Security Center Басқару сервері** түйінінде, **Кеңейтілген Бағдарламаны қашықтан жою** тапсырма түрін таңдаңыз.

   Жаңа тапсырма жасау шебері жұмысының нәтижесінде таңдалған құрылғылар жиынтығы үшін таңдалған бағдарламаны қашықтан жою тапсырмасы жасалады. Жасалған тапсырма **Тапсырмалар** қалтасының жұмыс аймағында көрсетіледі.

3. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан жою тапсырмасын жою нәтижесінде таңдалған бағдарлама таңдалған құрылғылардан жойылады.

Орнату пакеттерімен жұмыс істеу

Қашықтан орнату тапсырмаларын жасау кезінде бағдарламаны орнатуға қажетті параметрлер жиынтығын қамтитын орнату пакеттері қолданылады.

Орнату пакеттерінде кілт файлы болуы мүмкін. Кілт файлы бар орнату пакеттерін жалпыға ортақ қолжетімділікпен орналастыру ұсынылмайды.

Бір орнату пакетін көп рет қолдануыңызға болады.

Басқару сервері жасаған орнату пакеттері **Қашықтан орнату** қалтасындағы консоль тармағында, **Орнату пакеттері** ішкі қалтасына жіберілді. Басқару серверінде, орнату пакеттері Packages қызметтік қалтасында белгіленген ортақ қатынасы бар қалтада сақталады.

Қажет болса, Нысанды жою мақаласындағы нұсқауларды орындап, **Орнату пакеттері** ішкі қалтасынан орнату пакетін жоюға болады.

Ортақ қалтадағы орнату пакеттерінің мазмұнын қолмен өзгертпеңіз. Қажет болса, орнату пакетінің көшірмесін жасауға, қажетті өзгерістер енгізуге және жаңа орнату тапсырмаларын жасауға болады.

Орнату пакетін жасау

Бұл бөлімде орнату пакеттерінің келесі түрлерін жасау процедурасы сипатталған:

- Kaspersky бағдарламасының орнату пакеті;
- көрсетілген орындалатын файлдың орнату пакеті;
- Kaspersky дерекқорындағы бағдарламаның орнату пакеті.

Желілік агентті қашықтан орнатуға арналған орнату пакетін қолмен жасаудың қажеті жоқ. Ол Kaspersky Security Center бағдарламасын орнатқан кезде автоматты түрде қалыптасады және **Орнату пакеттері** қалтасында орналасады. Желілік агентті қашықтан орнатуға арналған пакет жойылған болса, оны сипаттамасы бар файл ретінде қайта қалыптастыру үшін Kaspersky Security Center дистрибутивінің NetAgent қалтасында орналасқан nagent.kud файлын таңдауыңыз керек.

Орнату пакетін жасау үшін:

1. Қажетті Басқару серверіне қосыңыз.
2. Консоль ағашында **Кеңейтілген** → **Қашықтан орнату** → **Орнату пакеттері** қалтасын таңдаңыз.
3. Автономды орнату пакетін жасау процесін келесі тәсілдердің көмегімен іске қосыңыз:
   - **Орнату пакеттері** қалтасының контекстік мәзірінде **Жаңа** → **Орнату пакеті** тармағын таңдаңыз.
   - Орнату пакеттерінің бос тізімінің контекстік мәзірінде **Жаңа** → **Орнату пакеті** тармағын таңдаңыз.
   - Орнату пакеттері тізімін басқару блогындағы **Орнату пакетін жасау** сілтемесіне өтіңіз.

   Орнату пакетін жасау шебері іске қосылады.
4. Сәйкес белгішені басу арқылы орнату пакеттерінің келесі түрлерінің бірін таңдаңыз:
   - Kaspersky бағдарламасының орнату пакеті.
   - Көрсетілген орындалатын файлдың орнату пакеті.
   - Kaspersky дерекқорындағы бағдарламаның орнату пакеті.
5. Жасалатын орнату пакетінің атауын көрсетіңіз.

   Кез келген атауды көрсетуге болады.
6. Келесі жолдардың бірімен орнату пакетін жасағыңыз келетін бағдарламаны немесе орындалатын файлды таңдаңыз:
   - **Шолу** түймесін басыңыз және стандартты **Ашу** терезесінде қолжетімді дискілерде орналасқан қажетті бағдарламаның дистрибутивін таңдаңыз.

     Бұл опция Kaspersky бағдарламасы немесе көрсетілген орындалатын файл үшін орнату пакетін жасауды таңдаған жағдайда қолданылады.

- **Шолу** түймесін басып, **Бағдарламаны таңдау** терезесінде қажетті бағдарламаның дистрибутивін таңдаңыз.

  Бұл опция Kaspersky дерекқорындағы бағдарлама үшін орнату пакетін жасауды таңдаған жағдайда қолданылады.

Басқару сервері үшін орнату пакетін жасап жатсаңыз, sc.kud файлын таңдаңыз. sc.kud файлы Kaspersky Security Center дистрибутивінің түбірлік қалтасында орналасқан.

Орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетпеңіз.

7. Лицензиялық келісім мен Құпиялық саясатымен танысыңыз.

   Бағдарламаның орнату пакетін жасаған кезде сізден сол бағдарламаның Лицензиялық келісімі мен Құпиялық саясатын қарап шығу және қабылдау сұралуы мүмкін.

   Екі құжатты да оқыңыз. Лицензиялық келісімнің және Құпиялық саясатының барлық шартына келіссеңіз, оларды тиісті жалаушаларды белгілеу арқылы қабылдаңыз.

   Бағдарламаны құрылғыңызға орнату жалғасады және орнату пакетін жасау қалпына келеді.

   Kaspersky Endpoint Security for Mac бағдарламасының орнату пакетін жасасаңыз, Лицензиялық келісім мен Құпиялық саясатының тілін таңдауға болады.

8. Қажет болса, жүйе құрамдастарын автоматты түрде орнатуды қосыңыз.

   Kaspersky дерекқорындағы бағдарламаларды орнату пакетін жасасаңыз, қажетті жүйе құрамдастарын автоматты түрде орнатуды қосуға болады. Орнату пакетін жасау шебері таңдалған бағдарлама үшін барлық мүмкін жалпыжүйелік құрамдастардың тізімін көрсетеді. Кейінірек бұл тізіммен орнату пакетінің сипаттарында таныса аласыз.

   Патчтың орнату пакетін жасасаңыз, тізім сол патчты енгізу үшін қажетті барлық жүйе құрамдасын қамтиды.

9. Пакет жасауды аяқтау үшін **Аяқтау** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін, жасалған орнату пакеті **Орнату пакеттері** қалтасының жұмыс аймағында көрсетіледі.

Автономды орнату пакетін жасау

Сіз және сіздің ұйымыңыздағы құрылғы пайдаланушылары бағдарламаларды құрылғыларға қолмен орнату үшін жеке орнату пакеттерін пайдалана аласыз.

Жеке орнату пакеті, Веб-серверге, ортақ қатынасы бар қалтаға орналастыруға немесе клиент құрылғысына басқа тәсілмен жіберуге болатын орындалатын файл (installer.exe) болып саналады. Жеке орнату пакетіне сілтемені электрондық пошта арқылы жіберуге де болады. Қолданбаны Kaspersky Security Center қатысуынсыз орнату үшін клиент құрылғысында алынған файлды жергілікті түрде іске қоса алады.

Жеке орнату пакетінің авторизацияланбаған тұлғаларға қолжетімді емес екеніне көз жеткізіңіз.

Kaspersky бағдарламалары үшін де, Windows, macOS және Linux үшін үшінші тарап бағдарламалары үшін де жеке орнату пакеттерін жасай аласыз. Үшінші тарап бағдарламаларына арналған жеке орнату пакетін жасау үшін, алдымен пайдаланушы орнату пакетін жасау керек.

Жеке орнату пакеттерін жасау көзі, Басқару серверінде жасалған тізімдегі орнату пакеттері болып табылады.

Жеке орнату пакетін жасау үшін:

1. Консоль ағашынан **Басқару сервері → Кеңейтілген → Қашықтан орнату → Орнату пакеттері** түйінін таңдаңыз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. Орнату пакеттері тізімінен автономды пакет жасауды қажет ететін орнату пакетін таңдаңыз.

3. Мәнмәтіндік мәзірде **Жеке орнату пакетін жасау** тармағын таңдаңыз.

   Нәтижесінде, автономды орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

4. Шебердің бірінші бетінде, егер сіз Kaspersky бағдарламасы үшін орнату пакетін таңдасаңыз және таңдалған бағдарламамен бірге Желілік агент орнатқыңыз келсе, **Желілік агентті осы бағдарламамен бірге орнату** параметрі қосулы екеніне көз жеткізіңіз.

   Әдепкі бойынша, параметр қосулы. Құрылғыда Желілік агенттің орнатылғанына сенімді болмасаңыз, осы параметрді қосу ұсынылады. Желілік агент құрылғыда бұрыннан орнатылған болса, онда Желілік агентпен бірге жеке орнату пакетін орнатқаннан кейін, Желілік агент ең жаңа нұсқасына дейін жаңартылатын болады.

   Осы параметрді өшіретін болсаңыз, Желілік агент құрылғыға орнатылмайды және құрылғы басқарылатын болмайды.

   Егер таңдалған бағдарлама үшін жеке орнату пакеті Басқару серверінде бұрыннан бар болса, шебер бұл туралы хабарды көрсетеді. Бұл жағдайда, келесі әрекеттердің бірін таңдауыңыз керек:

   - **Жеке орнату пакетін жасау**. Қолданбаның жаңа нұсқасы үшін жеке орнату пакетін жасаңыңыз келсе және сіз бұған дейін жасаған қолданбаның алдыңғы нұсқасы үшін жеке орнату пакетін қалдырғыңыз келсе, осы опцияны таңдаңыз. Жаңа жеке орнату пакеті басқа қалтада орналасқан.

   - **Бар жеке орнату пакетін пайдалану**. Бар жеке орнату пакетін пайдалануды қаласаңыз, осы параметрді таңдаңыз. Пакет жасау процесі іске қосылмайды.

   - **Бұрыннан бар жеке орнату пакетін қайта құрастыру**. Дәл осы бағдарлама үшін жеке орнату пакетін тағы да жасағыңыз келсе, осы параметрді таңдаңыз. Жеке орнату пакеті дәл осы қалтада орналастырылады.

5. Шебердің келесі бетінде **Тағайындалмаған құрылғыларды осы топқа жылжыту** параметрін таңдап, оларға Желілік агент орнатқаннан кейін клиент құрылғыларын жылжытқыңыз келетін басқару тобын көрсетіңіз.

   Әдепкі бойынша, құрылғылар **Басқарылатын құрылғылар** тобына жылжытылады.

   Желілік агентті орнатқаннан кейін, клиент құрылғысын қандай да бір басқару тобына жылжытқыңыз келмесе, **Құрылғыларды жылжытпау** параметрін таңдаңыз.

6. Шебердің келесі бетінде, жеке орнату пакетін жасау процесі аяқталғаннан кейін жеке орнату пакетін жасау нәтижесі және оған апаратын жол көрсетіледі.

   Сілтемелерден өтіп, келесі әрекеттерді орындауға болады:

   - Жеке орнату пакеті бар қалтаны ашу.

   - Жасалған жеке орнату пакетіне сілтемені электрондық пошта арқылы жіберіңіз. Ол үшін электрондық поштамен жұмыс істеуге арналған бағдарламаны іске қосу қажет.

   - Сілтемені веб-сайтқа орналастыру үшін HTML кодының үлгісін көшіріп алу. Мәтіндік файл (TXT пішімінде) TXT пішімімен байланысты бағдарлама арқылы жасалады және ашылады. Файлда атрибуттары бар <a> HTML-тегі көрсетіледі.

7. Егер сіз жеке орнату пакеттерінің тізімін ашқыңыз келсе, шебердің келесі бетінде **Автономды пакеттер тізімін ашу** параметрін қосыңыз.

8. **Дайын** түймесін басыңыз.

   Автономды орнату пакетін жасау шебері жабылады.

Жеке орнату пакеті жасалып, Басқару серверінің ортақ қатынасы бар қалтасының PkgInst салынған қалтасына орналастырылған. Орнату пакеттері тізімінің үстінде орналасқан **Автономды пакеттердің тізімін көру** түймесін басып, жеке орнату пакеттері тізімін қарап шыға аласыз.

Пайдаланушы орнату пакетін жасау

Сіз конфигурацияланған орнату пакеттерін пайдалана аласыз:

- клиент құрылғыларына кез келген бағдарламаны (мысалы, мәтіндік редактор) орнату, мысалы, тапсырманың көмегімен;
- жеке орнату пакетін жасау.

Пайдаланушы орнату пакеті – бұл файлдар жиынтығы бар қалта. Таңдаулы орнату пакетін жасау көзі – *мұрағаттық файл* болып табылады. Мұрағаттық файлда пайдаланушы орнату пакетіне қосылуы керек файл немесе файлдар бар. Пайдаланушы орнату пакетін жасай отырып, сіз пәрмен жолының параметрлерін көрсете аласыз, мысалы, бағдарламаны тыныш режимде орнату үшін.

Пайдаланушы орнату пакетін жасау үшін:

1. Консоль ағашында **Басқару сервері → Қосымша → Қашықтан орнату → Орнату пакеттері** тармағын таңдаңыз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. Орнату пакеттері тізімінің үстінен **Орнату пакетін жасау** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Шебердің бірінші бетінде **Көрсетілген орындалатын файл үшін орнату пакетін жасаңыз** параметрін таңдаңыз.

4. Шебердің келесі бетінде пайдаланушы орнату пакетінің атын көрсетіңіз.

5. Шебердің келесі бетінде, **Шолу** түймесін басыңыз және стандартты **Ашу** терезесінде, пайдаланушы орнату пакетін жасау үшін қолжетімді дискілерде орналасқан мұрағат файлын таңдаңыз.

   Сіз ZIP, CAB, TAR немесе TAR.GZ пішіміндегі мұрағаттық файлды жүктей аласыз. SFX (өздігінен шығарылатын мұрағат) файлынан орнату пакетін жасау мүмкін емес.

   Файлдар Kaspersky Security Center басқару серверіне жүктелген.

6. Шебердің келесі бетінде орындалатын файл үшін пәрмен жолының параметрлерін көрсетіңіз.

   Бағдарламаны орнату пакетінен тыныш режимде орнату үшін пәрмен жолының параметрлерін көрсетуге болады. Пәрмен жолының параметрлерін көрсету міндетті емес.

Қажет болса, келесі параметрлерді конфигурациялаңыз:

- **Бүкіл қалтаны орнату пакетіне көшіру**

  Егер орындалатын файл бағдарламаны орнатуға қажетті қосымша файлдармен бірге жүрсе, осы параметрді таңдаңыз. Бұл параметрді қоспас бұрын, барлық қажетті файлдардың бір қалтада сақталғанына көз жеткізіңіз. Егер бұл параметр қосылса, бағдарлама орнату пакетіне қалтаның барлық ішіндегісін, соның ішінде көрсетілген орындалатын файлды қосады.

- **Параметрлерді Kaspersky Security Center нұсқасы анықтай алатын бағдарламалар үшін ұсынылатын мәндерге түрлендіру**

  Егер аталған бағдарлама туралы ақпарат Kaspersky дерекқорында болса, бағдарлама ұсынылған параметрлермен орнатылады.

  Егер сіз **Орындалатын файлдың пәрмен жолы** өрісіне параметрлерді енгізсеңіз, олар ұсынылған параметрлерге өзгертіледі.

  Әдепкі бойынша, параметр қосулы.

  Kaspersky дерекқорын Kaspersky талдаушылары құрды және қолдайды. Дерекқорға қосылатын әрбір бағдарлама үшін Kaspersky талдаушылары орнатудың оңтайлы параметрлерін анықтайды. Параметрлер, клиент құрылғысына бағдарламаны қашықтан сәтті орнатуды қамтамасыз ететіндей етіп анықталады. Дерекқор Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын іске қосу кезінде автоматты түрде жаңартылады.

Пайдаланушы орнату пакетін жасау процесі басталады.

Шебер терезесінде процестің аяқталуы туралы ақпарат көрсетіледі.

Егер пайдаланушы орнату пакеті жасалмаса, тиісті хабарландыру көрсетіледі.

7. Шебер терезесін жабу үшін **Дайын** түймесін басыңыз.

Жасалған орнату пакеті Басқару серверінің ортақ қатынасы бар қалтасының Packages салынған қалтасына жүктеледі. Жүктелгеннен кейін, пайдаланушы орнату пакеті орнату пакеттерінің тізімінде пайда болады.

Басқару серверіндегі орнату пакеттерінің тізімінде пайдаланушы орнату пакетінің сипаттарын көруге және өзгертуге болады.

Пайдаланушы орнату пакеттерінің сипаттарын қарап шығу және өзгерту

Пайдаланушы орнату пакетін жасағаннан кейін, сипаттар терезесінде ол туралы жалпы ақпаратты көруге және орнату параметрлерін көрсетуге болады.

Пайдаланушы орнату пакетінің сипаттарын көру және өзгерту үшін:

1. Консоль ағашында **Басқару сервері → Қосымша → Қашықтан орнату → Орнату пакеттері** тармағын таңдаңыз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. Орнату пакетінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Таңдалған орнату пакеті сипаттары терезесі ашылады.

3. Келесі ақпарат көрсетіледі:

- Орнату пакетінің атауы
- Пайдаланушы орнату пакетіне қапталған бағдарламаның атауы
- Бағдарлама нұсқасы
- Орнату пакетін жасау күні
- Басқару серверіндегі пайдаланушы орнату пакетіне апаратын жол
- Орындалатын файлды іске қосу параметрлері

4. Келесі параметрлерді белгілеңіз:

- Орнату пакетінің атауы
- **Қажетті жалпы жүйелік құрамдастарды орнату**

  Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

  Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

  Әдепкі бойынша, параметр өшірулі.

  > Бұл параметр, орнату пакетіне қосылған бағдарламаны Kaspersky Security Center таныған жағдайда ғана қолжетімді.

- **Орындалатын файлдың пәрмен жолы**

  Егер бағдарлама хабарларды көрсетпестен орнату үшін қосымша параметрлерді қажет етсе, оларды осы өрісте көрсетіңіз. Қосымша ақпарат алу үшін өндірушінің құжаттамасын қараңыз.

  Сіз басқа параметрлерді де көрсете аласыз.

  > Бұл параметр тек Kaspersky бағдарламалары негізінде жасалмаған пакеттер үшін қолжетімді.

5. Өзгерістерді сақтау үшін **OK** немесе **Қолдану** түймесін басыңыз.

Жаңа параметрлер сақталды.

Kaspersky Security Center жеткізу жиынтығындағы Желілік агенттің орнату пакетін алу

Сіз Kaspersky Security Center орнату қажеттілігінсіз Kaspersky Security Center жеткізу жиынтығынан Желілік агенттің орнату пакетін ала аласыз. Содан кейін, Желілік агентті клиент құрылғыларына орнату үшін орнату пакетін пайдалануға болады.

Kaspersky Security Center жеткізу жиынтығындағы Желілік агенттің орнату пакетін алу үшін:

1. Kaspersky Security Center дистрибутивінен ksc_<нұсқа нөмірі>.<жинақ нөмірі>_full_<локализация тілі> .exe орындалатын файлын іске қосыңыз.
2. Пайда болған терезеде **Орнату пакеттерін шығарып алу** сілтемесінен өтіңіз.
3. Орнату пакеттері тізімінде Желілік агенттің орнату пакетінің жанына жалаушаны қойып, **Келесі** түймесін басыңыз.
4. Қажет болса, орнату пакетін алып шығару үшін көрсетілетін қалтаны өзгерту мақсатында **Шолу** түймесін басыңыз.
5. **Шығарып алу** түймесін басыңыз.

   Бағдарлама Желілік агенттің орнату пакетін алып шығарады.
6. Процесс аяқталғаннан кейін, **Жабу** түймесін басыңыз.

Желілік агенттің орнату пакеті таңдалған қалтаға мұрағаттан шығарылады.

Орнату пакетінің көмегімен сіз Желілік агентті келесі тәсілдердің бірімен орната аласыз:

- Алып шығарылған қалтадан setup.exe файлын жергілікті түрде іске қосу арқылы.
- Автоматты орнату көмегімен.
- Microsoft Windows топтық саясаттары тетігінің көмегімен.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату

Орнату пакеттерін қосалқы Басқару серверлеріне тарату үшін:

1. Өзіңізге қажетті қосалқы Басқару серверлерін басқаратын Басқару серверіне қосылыңыз.
2. Келесі тәсілдердің бірімен орнату пакетін қосалқы Басқару серверлеріне тарату тапсырмасын құруды бастаңыз:

   - Егер сіз таңдалған басқару тобының қосалқы Серверлері үшін тапсырма жасағыңыз келсе, сол топ үшін топтық тапсырма құруды бастаңыз.
   - Егер сіз қосалқы Серверлер жиынтығы үшін тапсырма жасағыңыз келсе, құрылғылар жиынтығы үшін тапсырма құруды бастаңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде, **Kaspersky Security Center Басқару сервері** түйінінде, **Кеңейтілген** қалтасында **Орнату пакетін тарату** тапсырма түрін таңдаңыз.

Жаңа тапсырма жасау шебері жұмысының нәтижесінде таңдалған қосалқы Басқару серверлеріне таңдалған орнату пакеттерін тарату тапсырмасы жасалады.

3. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Тапсырманы орындау нәтижесінде, таңдалған орнату пакеттері таңдалған қосалқы Басқару серверлеріне көшіріледі.

Орнату пакеттерін тарату нүктелері көмегімен тарату

Басқару тобы шегінде орнату пакеттерін тарату үшін тарату нүктелерін пайдалануға болады.

Басқару серверінен орнату пакеттерін алғаннан кейін, тарату нүктелері оларды көпмекенжайлы IP жіберілімі арқылы клиент құрылғыларына автоматты түрде таратады. Басқару тобы шегінде жаңа орнату пакеттерін IP-тарату бір рет жүргізіледі. Егер тарату кезінде клиент құрылғысы ұйымның желісінен ажыратылған болса, онда орнату тапсырмасын іске қосқан кезде клиент құрылғысының Желілік агенті тарату нүктесінен қажетті орнату пакетін автоматты түрде жүктейді.

Kaspersky Security Center-ге бағдарламаны орнату нәтижелері туралы ақпаратты жіберу

Бағдарламаның орнату пакетін жасағаннан кейін, сіз орнату пакетін, бағдарламаны орнату нәтижелері туралы диагностикалық ақпарат Kaspersky Security Center бағдарламасына жіберілетіндей етіп конфигурациялай аласыз. Kaspersky бағдарламаларының орнату пакеттері үшін бағдарламаны орнату нәтижесі туралы диагностикалық ақпаратты беру әдепкі бойынша конфигурацияланған, қосымша конфигурациялау қажет емес.

Бағдарламаны орнату нәтижесі туралы диагностикалық ақпаратты Kaspersky Security Center бағдарламасына жіберуді конфигурациялау үшін:

1. Таңдалған бағдарлама үшін Kaspersky Security Center құралдары құрған орнату пакетінің қалтасына өтіңіз. Бұл қалта Kaspersky Security Center орнату кезінде көрсетілген ортақ қатынасы бар қалтада орналасқан.

2. Өңдеу үшін kpd немесе kud кеңейтімі бар файлды ашыңыз (мысалы, Microsoft Windows "Блокнот" мәтіндік редакторы арқылы).

   Файл кәдімгі конфигурациялық ini файлы пішіміне ие.

3. Файлға келесі жолдарды қосыңыз:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Бұл пәрмен Kaspersky Security Center бағдарламасын, орнату пакеті құрылған бағдарламаны орнатудың аяқталуын күтетін және орнату бағдарламасының қайтару кодын талдайтындай етіп конфигурациялайды. Диагностикалық ақпаратты беруді өшіру қажет болса, Wait кілті үшін 0 мәнін белгілеңіз.

4. Сәтті орнатудың қайтару кодтарының сипаттамасын енгізіңіз. Ол үшін файлға келесі жолдарды қосыңыз:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

Міндетті емес кілттер төртбұрышты жақшада берілген.

Жолдар синтаксисі:

- `<return code>`. Орнату бағдарламасының қайтару кодына сәйкес келетін кез келген сан. Қайтару кодтарының саны ерікті болуы мүмкін.
- `<description>`. Орнату нәтижесінің мәтіндік сипаттамасы. Сипаттама болмауы мүмкін.

5. Қате аяқталған орнату үшін қайтару кодтарының сипаттамасын енгізіңіз. Ол үшін файлға келесі жолдарды қосыңыз:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   Жол синтаксисі сәтті орнатылған кезде қайтару кодтарының жол синтаксисіне сәйкес келеді.

6. Енгізілген өзгертулерді сақтай отырып, kpd немесе kud файлын жабыңыз.

Пайдаланушы көрсеткен бағдарламаны орнату нәтижелері туралы ақпарат Kaspersky Security Center журналына жазылады және оқиғалар тізімінде, есептерде және тапсырмаларды орындау нәтижелерінде көрсетіледі.

Орнату пакеттері үшін KSN прокси-сервері мекенжайын анықтау

Басқару серверінің мекенжайы немесе домені өзгерген жағдайда, сіз орнату пакеті үшін KSN прокси-серверінің мекенжайын көрсете аласыз.

Орнату пакетіне арналған KSN прокси-сервері мекенжайын анықтау үшін:

1. **Қашықтан орнату** қалтасындағы консоль ағашында тінтуірді екі рет нұқып, **Орнату пакеттері** салынған қалтасын басыңыз.
2. Пайда болған терезеде **Сипаттар** түймесін басыңыз.
3. Ашылған сипаттар терезесінде **Жалпы** бөлікшесін таңдаңыз.
4. Сипаттар терезесінің **Жалпы** бөлікшесінде KSN прокси-сервері мекенжайын енгізіңіз.

Орнату пакеттері осы мекенжайы әдепкі бойынша қолданатын болады.

Бағдарламалардың өзекті нұсқаларын алу

Kaspersky Security Center бағдарламасы Kaspersky серверлерінде сақталатын корпоративтік бағдарламалардың өзекті нұсқаларын алуға мүмкіндік береді.

Kaspersky корпоративтік бағдарламаларының өзекті нұсқаларын алу үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар түйінді таңдап, **Мониторинг** қойыншасында, **Орналастыру** бөлімінде **Мұнда Kaspersky бағдарламаларының қолжетімді жаңа нұсқалары бар** сілтемесінен өтіңіз.

     Мұнда Kaspersky бағдарламаларының қолжетімді жаңа нұсқалары бар сілтемесі Басқару сервері Kaspersky интернет-серверінде корпоративтік бағдарламаның кезекті нұсқасын анықтаған кезде қолжетімді болады.

   - Консоль ағашында **Кеңейтілген** → **Қашықтан орнату** → **Орнату пакеттері** тармағын таңдап, жұмыс аймағында **Қосымша әрекеттер** түймесін басып, ашылмалы тізімнен **Kaspersky бағдарламаларының ағымдағы нұсқаларын көру** тармағын таңдаңыз.

   Kaspersky бағдарламаларының ағымдағы нұсқаларының тізімі пайда болады.

2. Қажетті бағдарламаны табуды жеңілдету үшін Kaspersky бағдарламаларының тізімін сүзуге болады.

   Бағдарламалар тізімін келесі критерийлер бойынша сүзу үшін **Ағымдағы бағдарлама нұсқалары** терезесінің жоғарғы жағында **Сүзгі** сілтемесінен өтіңіз:

   - **Құрамдастар**. Бұл критерийді желіде қолданылатын қорғаныс аумақтары бойынша Kaspersky бағдарламаларының тізімін сүзу үшін пайдаланыңыз.
   - **Жүктеп алынатын бағдарламалық жасақтаманың түрі**. Бұл критерийді Kaspersky бағдарламалар тізімін бағдарлама түріне қарай сүзу үшін пайдаланыңыз.
   - **Қандай жаңартулар мен бағдарламалық жасақтаманы көрсету керек**. Бұл критерийді қолжетімді Kaspersky бағдарламаларын белгілі бір нұсқалар бойынша көрсету үшін пайдаланыңыз.
   - **Бағдарламалық жасақтаманы және жаңартуларды қандай тілдерде көрсету керек**. Бұл критерийді белгілі бір локализация тілі бар Kaspersky бағдарламаларын көрсету үшін пайдаланыңыз.

   Өзгерістерді қолдану үшін **Қолдану** түймесін басыңыз.

3. Тізімнен қажетті бағдарламаны таңдаңыз.

4. Бағдарламаның дистрибутивін **Дистрибутивтің веб-мекенжайы** жолындағы сілтеме арқылы жүктеңіз.

   Басқарылатын бағдарламаларды жаңарту үшін Kaspersky Security Center бағдарламасының белгілі бір ықшам нұсқасын орнату қажет болуы мүмкін. Бұл нұсқа сіздің қазіргі нұсқаңыздан да соңғы болса, бұл жаңартулар көрсетілсе де, оларды мақұлдау мүмкін емес. Сондай-ақ, Kaspersky Security Center жаңартпайынша, осындай жаңартулардан орнату пакеттерін жасау мүмкін емес. Сізге Kaspersky Security Center данасын қажетті ықшам нұсқаға дейін жаңарту ұсынылады.

Таңдалған бағдарлама үшін **Бағдарламаларды жүктеп алу және орнату пакеттерін жасау** түймесі көрсетілсе, сіз бағдарлама дистрибутивін жүктеу және орнату пакетін автоматты түрде жасау үшін осы түймені баса аласыз. Бұл жағдайда, Kaspersky Security Center бағдарламаның дистрибутивін Басқару серверіне Kaspersky Security Center орнату кезінде белгіленген ортақ қатынасы бар қалтаға жүктейді. Автоматты түрде жасалған орнату пакеттері тізімі **Қашықтан орнату** консоль ағашы қалтасында, **Орнату пакеттері** салынған қалтасында көрсетіледі.

Ағымдағы бағдарлама нұсқалары терезесі жабылғаннан кейін, **Мұнда Kaspersky бағдарламаларының қолжетімді жаңа нұсқалары бар** сілтемесі **Орналастыру** бөлімінен алынып тасталады.

Сіз бағдарламалардың жаңа нұсқаларының орнату пакеттерін жасай аласыз және консоль ағашының **Қашықтан орнату** қалтасында, **Орнату пакеттері** ішкі қалтасында жасалған орнату пакеттермен жұмыс жасай аласыз.

Сондай-ақ, сіз **Орнату пакеттері** қалтасының жұмыс аймағындағы **Kaspersky бағдарламаларының ағымдағы нұсқаларын көру** сілтемесі арқылы **Ағымдағы бағдарлама нұсқалары** терезесін аша аласыз.

Windows басқаратын құрылғыны қашықтан орнатуға дайындау

Клиент құрылғысына бағдарламаны қашықтан орнату келесі себептерге байланысты қатемен аяқталуы мүмкін:

- Тапсырма бұған дейін осы құрылғыда сәтті орындалды.

  Бұл жағдайда, оны қайта орындау қажет емес.

- Тапсырманы іске қосу кезінде құрылғы өшірілді.

  Бұл жағдайда, құрылғыны қосып, тапсырманы қайтадан іске қосу қажет.

- Клиент құрылғысында орнатылған Басқару сервері мен Желілік агент арасында байланыс жоқ.

  Мәселенің себебін анықтау үшін клиент құрылғысын қашықтан диагностикалау утилитасын (klactgui) пайдалануыңызға болады.

- Құрылғыда желілік агент орнатылмаған болса, қашықтан орнату кезінде келесі мәселелер туындауы мүмкін:

  - Клиент құрылғысында **Файлдарға қарапайым жалпы қатынасты өшіру** орнатылған.
  - Клиент құрылғысында Server қызметі жұмыс істемейді.
  - Клиент құрылғысында қажетті порттар жабық.
  - Тапсырма орындалып жатқан есептік жазбаның құқықтары жеткіліксіз.

  Қолданбаны желілік агент орнатылмаған клиент құрылғысына орнату кезінде туындауы мүмкін мәселелерге жол бермеу үшін Kaspersky Security Center қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру процедурасында сипатталғандай әрекет ету керек.

Бұрын riprep утилитасы құрылғыны қашықтан орнатуға дайындау үшін пайдаланылды. Бұл енді операциялық жүйелерді реттеудің ескірген әдісі болып саналады. Riprep утилитасын Windows XP және Windows Server 2003 R2 нұсқасынан жаңа операциялық жүйелерде пайдалану ұсынылмайды.

Linux операциялық жүйесімен жұмыс істейтін құрылғыны дайындау және Linux операциялық жүйесі бар құрылғыға Желілік агентті қашықтан орнату

Желілік агентті орнату екі қадамнан тұрады:

- Linux операциялық жүйесі бар құрылғыны дайындау
- Желілік агентті қашықтан орнату

Linux операциялық жүйесі бар құрылғыны дайындау

Linux операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау үшін:

1. Linux Желілік агентін орнатқыңыз келетін құрылғыда қолдау көрсетілетін Linux дистрибутивтерінің бірі жұмыс істейтініне көз жеткізіңіз.
2. Бағдарлама интерфейсін пайдаланып немесе Kaspersky веб-сайтынан желілік агентті орнату пакетін жүктеп алыңыз.
3. Linux операциялық жүйесі бар мақсатты құрылғыда келесі бағдарламалық жасақтама орнатылғанына көз жеткізіңіз:
   - Sudo (Ubuntu 10.04 үшін Sudo нұсқасы — 1.7.2p1 немесе одан кейінгі)
   - Perl тілі интерпретаторының 5.10 немесе одан жоғары нұсқасы
   - ps утилитасы
4. Құрылғының конфигурациясын тексеріңіз:
   a. Құрылғыға SSH арқылы қосылуға болатындығын тексеріңіз (мысалы, PuTTY бағдарламасы).

      Құрылғыға қосыла алмасаңыз, `/etc/ssh/sshd_config` файлын ашып, келесі параметрлердің төмендегі мәні бар екеніне көз жеткізіңіз:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      Құрылғыға қиындықсыз қосыла алсаңыз, /etc/ssh/sshd_config файлын өзгертпеңіз; әйтпесе қашықтан орнату тапсырмасын орындау кезінде SSH түпнұсқалық растама қатесіне тап болуыңыз мүмкін.

      `sudo service ssh restart` пәрменін қолдана отырып, файлды сақтаңыз (қажет болса) және SSH қызметін қайта іске қосыңыз.

   b. Linux негізіндегі тағайындалмаған құрылғыда TCP 22 портының ашық және қолжетімді екеніне көз жеткізіңіз. Linux үшін Желілік агентті сәтті орнату үшін TCP 22 порты қолжетімді болуы керек.

c. Құрылғы қосылатын пайдаланушы есептік жазбасы үшін sudo құпия сөзін өшіріңіз.

d. sudoers конфигурациялық файлын ашу үшін sudo `visudo` пәрменін қолданыңыз.

Сіз ашқан файлда файлдың соңына келесі жолды қосыңыз: <`пайдаланушы аты`> `ALL = (ALL) NOPASSWD: ALL`. Бұл жағдайда, <`пайдаланушы аты`> — SSH протоколы арқылы құрылғыға қосылу үшін пайдаланылатын пайдаланушы есептік жазбасы. Astra Linux операциялық жүйесін пайдалансаңыз, соңғы жолды /etc/sudoers файлына келесі мәтінмен қосыңыз: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. sudoers файлын сақтаңыз және жабыңыз.

f. SSH арқылы құрылғыға қайта қосылыңыз және `sudo whoami` пәрменінің көмегімен, sudo қызметі құпиясөзді қажет етпейтінін тексеріңіз.

5. `/etc/systemd/logind.conf` файлын ашыңыз және келесі әрекеттердің бірін орындаңыз:

- KillUserProcesses параметрі үшін "no" мәнін көрсетіңіз: `KillUserProcesses=no`.
- KillExcludeUsers параметрі үшін, қашықтан орнату орындалатын есептік жазбаның пайдаланушы атауын енгізіңіз, мысалы, `KillExcludeUsers=root`.

Егер мақсатты құрылғы Astra Linux басқаруымен жұмыс істеп тұрса, `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` экспорттау жолын `/home/<пайдаланушы аты>/.bashrc` файлына қосыңыз, мұндағы <`пайдаланушы аты`> – SSH арқылы құрылғыны қосу үшін пайдаланылатын пайдаланушы есептік жазбасы.

Өзгертілген параметрді қолдану үшін, Linux басқаруымен жұмыс істейтін құрылғыны қайта іске қосыңыз немесе келесі пәрменді іске қосыңыз:

```
sudo systemctl restart systemd-logind.service
```

6. SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

7. Жабық бағдарлама ортасы режимінде жұмыс істейтін Astra Linux операциялық жүйесі жұмыс істейтін құрылғыларға Желілік агентті орнатқыңыз келсе, Astra Linux құрылғыларын дайындау үшін қосымша қадамдарды орындаңыз.

8. Желілік агентті RED OS 7.3.4 не одан кейінгі нұсқадағы немесе MSVSPHERE 9.2 не одан кейінгі нұсқадағы операциялық жүйені қолданатын құрылғыларға орнатқыңыз келсе, желілік агенттің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

Желілік агентті қашықтан орнату

Linux операциялық жүйесі бар құрылғыға Желілік агентті орнату үшін:

1. Орнату пакеттерін жүктеп алыңыз және жасаңыз:

a. Пакетті құрылғыға орнатпас бұрын, онда осы пакетке арналған тәуелділіктер (бағдарламалар, кітапханалар) орнатылғанына көз жеткізіңіз.

Пакет орнатылатын Linux дистрибутивіне тән утилиталарды қолдана отырып, әр пакетке арналған тәуелділіктерді өзіңіз қарап шыға аласыз. Утилиталар туралы ақпаратпен, өзіңіздің операциялық жүйеңізге қоса берілген құжаттамада таныса аласыз.

b. Қашықтан орнату пакетін жасау үшін келесі файлдарды пайдаланыңыз:

- klnagent.kpd;
- akinstall.sh;
- Желілік агенттің deb немесе rpm пакеті.

2. Бағдарламаны қашықтан орнату тапсырмасын келесі параметрлермен жасаңыз:

- Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Басқару сервері арқылы операциялық жүйенің құралдарымен** жалаушасын қойыңыз. Барлық басқа жалаушаларды алып тастаңыз.
- **Тапсырманы іске қосу үшін есептік жазбаны таңдау** бетінде, құрылғыға SSH арқылы қосылу мақсатымен пайдаланылатын есептік жазба параметрлерін көрсетіңіз.

3. Бағдарламаны қашықтан орнату тапсырмасын іске қосыңыз. Қоршаған ортаны сақтау үшін `su` пәрменіне арналған параметрді пайдаланыңыз: `-m, -p, --preserve-environment`.

SUSE Linux Enterprise Server 15 басқаратын құрылғыны Желілік агентті орнатуға дайындау

SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыға Желілік агентті орнату үшін,

Желілік агентті орнатпас бұрын келесі пәрменді іске қосыңыз:

```
sudo zypper install insserv-compat
```

Бұл сізге insserv-compat пакетін орнатуға және Желілік агентті дұрыс конфигурациялауға мүмкіндік береді.

> Пакеттің бұған дейін орнатылғанан тексеру үшін `rpm -q insserv-compat` пәрменін орындаңыз.

Егер сіздің желіңізде SUSE Linux Enterprise Server 15 жұмыс істейтін көптеген құрылғылар болса, сіз компанияның инфрақұрылымын конфигурациялау және басқару үшін арнайы бағдарламалық жасақтаманы пайдалана аласыз. Осы бағдарламалық жасақтаманы пайдаланып, insserv-compact пакетін бірден барлық қажетті құрылғыларға автоматты түрде орнатуға болады. Мысалы, сіз Puppet, Ansible, Chef қолдана аласыз немесе скриптті өзіңізге ыңғайлы етіп жасай аласыз.

Құрылғыда SUSE Linux Enterprise үшін GPG қол қою кілттері болмаса, келесі ескертуді көруіңіз мүмкін: `Package header is not signed!` Ескертуді елемеу үшін `i` опциясын таңдаңыз.

insserv-compat пакетін орнатудан бөлек, сіздің Linux құрылғыларыңыз толығымен дайындалғанына көз жеткізіңіз. Содан кейін, Желілік агентті орналастырып, орнатыңыз.

macOS операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау

macOS операциялық жүйесі бар құрылғыны Желілік агентті қашықтан орнатуға дайындау үшін:

1. macOS операциялық жүйесі бар мақсатты құрылғыда sudo бағдарламасы орнатылғанына көз жеткізіңіз.

2. Құрылғының конфигурациясын тексеріңіз:

   a. Клиент құрылғысында 22-порттың ашық екеніне көз жеткізіңіз. Бұл үшін, **Жүйелік конфигурациялар** бөлімінде **Алмасу** тақтасын ашып, **Қашықтан кіру** жалаушасының қойылғанына көз жеткізіңіз.

   Сіз клиент құрылғысына Secure Shell (SSH) протоколы бойынша тек 22-порт арқылы қосыла аласыз. Сіз порт нөмірін өзгерте алмайсыз.

   macOS құрылғысына қашықтан кіру үшін `ssh <құрылғы_аты>` пәрменін қолдана аласыз. macOS құрылғысына қатынасуға рұқсат алған пайдаланушылардың әрекет ету аумағын белгілеу үшін **Ортақ қатынас** тақтасында **Қатынасты рұқсат ету** параметрін қолдана аласыз.

   b. Құрылғы қосылатын пайдаланушы есептік жазбасы үшін sudo құпия сөзін өшіріңіз.

   Терминалда sudoers конфигурациялық файлын ашу үшін `sudo visudo` пәрменін қолданыңыз. Сіз ашқан файлда, `Пайдаланушы артықшылықтары ерекшеліктері` өрісінде келесіні көрсетіңіз: `username ALL = (ALL) NOPASSWD: ALL`. Бұл жағдайда, `username` – құрылғыға SSH протоколы арқылы қосылу үшін қолданылатын пайдаланушы есептік жазбасы болып табылады.

   c. sudoers файлын сақтаңыз және жабыңыз.

   d. SSH арқылы құрылғыға қайта қосылыңыз және `sudo whoami` пәрменінің көмегімен, sudo қызметі құпиясөзді қажет етпейтінін тексеріңіз.

3. Орнату пакеттерін жүктеп алыңыз және жасаңыз:

   a. Желілік агенттің орнату пакетін келесі тәсілдердің бірімен жүктеп алыңыз:

   - Консоль ағашында, қолжетімді пакеттер ішінен таңдау үшін контекстік мәзірден **Қашықтан орнату** → **Орнату пакеттері** және одан кейін, **Ағымдағы бағдарлама нұсқаларын көрсету** таңдау арқылы
   - Желілік агенттің тиісті нұсқасын техникалық қолдау қызметінің https://support.kaspersky.com/ веб-сайтынан жүктеп алу арқылы
   - Техникалық қолдау қызметі мамандарынан орнату пакетін сұрау арқылы

   b. Қашықтан орнату пакетін жасау үшін келесі файлдарды пайдаланыңыз:

   - klnagent.kud
   - install.sh
   - klnagentmac.dmg

4. Бағдарламаны қашықтан орнату тапсырмасын келесі параметрлермен жасаңыз:

    - Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен** жалаушасын қойыңыз. Барлық басқа жалаушаларды алып тастаңыз.

    - **Тапсырманы іске қосу үшін есептік жазбаны таңдау** терезесінде, тапсырманы іске қосу үшін құрылғыға SSH арқылы қосылу мақсатымен пайдаланылатын есептік жазба параметрлерін көрсетіңіз.

Клиент құрылғысы сіз жасаған тиісті тапсырманы пайдаланып Желілік агентті қашықтан орнатуға дайын.

Kaspersky бағдарламасы: лицензиялау және белсендіру

Бұл бөлімде Kaspersky Security Center бағдарламасының Kaspersky басқарылатын бағдарламаларының лицензиялық кілттерімен жұмыс істеу мүмкіндіктері сипатталған.

Kaspersky Security Center бағдарламасы Kaspersky бағдарламаларының лицензиялық кілттерін клиент құрылғыларына орталықтан таратуға, кілттердің қолданылуын бақылау және лицензиялардың жарамдылық мерзімін ұзартуға мүмкіндік береді.

Kaspersky Security Center көмегімен лицензиялық кілт қосылған кезде лицензиялық кілттің сипаттары Басқару серверінде сақталады. Осы ақпарат негізінде бағдарлама лицензиялық кілттерді пайдалану туралы есепті қалыптастырады және әкімшіге лицензиялардың жарамдылық мерзімінің аяқталғаны және лицензиялық кілттердің сипаттарында қойылған лицензиялық шектеулердің асып кеткені туралы хабарлайды. Басқару сервері параметрлері құрамындағы лицензиялық кілттерді пайдалану туралы хабарландыру параметрлерін конфигурациялауға болады.

Басқарылатын бағдарламаларды лицензиялау

Басқарылатын құрылғыларда орнатылған Kaspersky бағдарламалары, бағдарламалардың әрқайсысына кілт файлын немесе белсендіру кодын қолдану арқылы іске қосылуы керек. Кілт файлы немесе белсендіру коды келесі тәсілдермен таратылуы мүмкін:

- Автоматты түрде тарату
- Басқарылатын бағдарламаның орнату пакетін пайдалану
- Басқарылатын бағдарламаның *Лицензиялық кілтін қосу* тапсырмасы арқылы
- Басқарылатын бағдарламаны қолмен белсендіру

Жоғарыда аталған тәсілдердің кез келгенімен белсенді немесе сақтық лицензиялық кілтті қосуға болады. Kaspersky бағдарламасы қазіргі уақытта белсенді болып саналатын кілтті пайдаланады және белсенді кілттің әрекет ету мерзімі аяқталғаннан кейін қолданылатын резервттегі лицензиялық кілтті сақтайды. Лицензиялық кілті қосылып жатқан бағдарлама кілттің белсенді немесе резервтік екенін анықтайды. Кілтті анықтау лицензиялық кілтті қосу үшін қолданылатын тәсілге байланысты емес.

Автоматты түрде тарату

Егер сіз әртүрлі басқарылатын бағдарламаларды қолдансаңыз және белгілі бір кілт файлын немесе белсендіру кодын құрылғыларға тарату маңызды болса, белсендіру кодын немесе кілтті таратудың басқа тәсілдерін қолданыңыз.

Kaspersky Security Center қолда бар лицензиялық кілттерді құрылғыларға автоматты түрде таратуға мүмкіндік береді. Мысалы, Басқару сервері қоймасында үш лицензиялық кілт бар. Барлық лицензиялық кілттер үшін **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасы қойылған. Ұйымның құрылғыларында Kaspersky қауіпсіздік бағдарламасы, мысалы, Kaspersky Endpoint Security for Windows орнатылған. Лицензиялық кілтті таратуды қажет ететін жаңа құрылғы табылды. Бағдарлама бұл құрылғыға не сәйкес келетінін анықтайды, мысалы, қоймадан екі лицензиялық кілт, *Кілт_1* лицензиялық кілті және *Кілт_2* лицензиялық кілті. Құрылғыға жарамды лицензиялық кілттердің бірі қолданылады. Бұл жағдайда, осы екі лицензиялық кілттің қайсысы осы құрылғыға қолданылатынын болжау мүмкін емес, өйткені лицензиялық кілттерді автоматты түрде тарату әкімшінің араласуын қамтымайды.

Лицензиялық кілтті құрылғыларға таратқан кезде осы лицензиялық кілт үшін құрылғылар есептеледі. Лицензиялық кілт қолданылатын құрылғылардың саны лицензиялық шектен аспайтынына көз жеткізуіңіз керек. Егер құрылғылардың саны лицензиялық шектен асып кетсе, мұндай құрылғыларға *Критикалық* күйі беріледі.

Таратпас бұрын, кілт файлы немесе белсендіру коды Басқару сервері қоймасына қосылуы керек.

Нұсқаулар:

- Басқару консолі:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті автоматты түрде тарату

  Немесе
- Kaspersky Security Center Web Console:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті автоматты түрде тарату

Келесі жағдайларда автоматты түрде таратылатын лицензиялық кілт виртуалды Басқару серверінің қоймасында көрінбеуі мүмкін екенін ескеріңіз:

- Лицензиялық кілт бағдарлама үшін жарамсыз.
- Виртуалды Басқару серверінде басқарылатын құрылғылар жоқ.
- Лицензиялық кілт басқа виртуалды Басқару сервері басқаратын құрылғылар үшін әлдеқашан қолданыста және құрылғылар санының лицензиялық шегіне жетті.

Басқарылатын бағдарламаның орнату пакетіне кілт файлын немесе белсендіру кодын қосу.

Қауіпсіздік тұрғысынан, бұл параметрді пайдалану ұсынылмайды. Орнату пакетіне қосылған кілт файлы немесе белсендіру коды бұзылуы мүмкін.

Басқарылатын бағдарламаны орнату пакеті арқылы орнатқан жағдайда, белсендіру кодын немесе кілт файлын орнату пакетінде немесе сол бағдарламаның саясатында көрсетуге болады. Лицензиялық кілт, құрылғыны Басқару серверімен кезекті рет синхрондау кезінде басқарылатын құрылғыларға қолданылады.

Нұсқаулар:

- Басқару консолі:
  - Орнату пакетін жасау
  - Клиент құрылғыларына бағдарламаларды орнату

  Немесе
- Kaspersky Security Center Web Console: Лицензиялық кілтті орнату пакетіне қосу.

Лицензиялы бағдарламалардың лицензиялық кілтін қосу тапсырмасы арқылы тарату

Басқарылатын бағдарламаның *Лицензиялық кілтін қосу* тапсырмасын пайдаланған жағдайда, сіз құрылғыларға таратылатын лицензиялық кілтті таңдап, құрылғыларды өзіңізге ыңғайлы тәсілмен таңдай аласыз, мысалы, басқару тобын немесе құрылғылар таңдауын таңдау арқылы.

Таратпас бұрын, кілт файлы немесе белсендіру коды Басқару сервері қоймасына қосылуы керек.

Нұсқаулар:

- Басқару консолі:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті клиент құрылғыларына тарату

  Немесе
- Kaspersky Security Center Web Console:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті клиент құрылғыларына тарату

Құрылғыларға белсендіру кодын немесе кілт файлын қолмен қосу.

Орнатылған Kaspersky бағдарламасын жергілікті түрде қосу үшін бағдарлама құралдарын пайдалануға болады. Кеңейтілген ақпаратты орнатылған бағдарламаларға арналған құжаттамадан қараңыз.

Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу

Пайдаланылған лицензиялық кілттер туралы ақпаратты қарап шығу үшін:

Консоль ағашында **Kaspersky лицензиялары** қалтасын таңдаңыз.

Қалтаның жұмыс аймағында клиент құрылғыларында қолданылатын лицензиялық кілттердің тізімі көрсетіледі.

Әрбір лицензиялық кілттің жанында оны пайдалану түріне сәйкес келетін белгіше көрсетіледі:

-  – пайдаланылған лицензиялық кілт туралы ақпарат Басқару серверіне қосылған клиент құрылғысынан алынған. Бұл лицензиялық кілттің файлы Басқару серверінде сақталмайды.
-  – лицензиялық кілт Басқару серверінің қоймасында орналасқан. Бұл лицензиялық кілтті автоматты түрде тарату өшірілген.
-  – лицензиялық кілт Басқару серверінің қоймасында орналасқан. Бұл лицензиялық кілтті автоматты түрде тарату қосылған.

Клиент құрылғысындағы бағдарламаны белсендіру үшін қандай лицензиялық кілттер қолданылатыны туралы ақпаратты клиент құрылғысының сипаттар терезесінің **Бағдарламалар** бөлімінен көре аласыз.

Виртуалды Басқару серверінің лицензиялық кілттерінің өзекті параметрлерін анықтау үшін Басқару сервері тәулігіне бір реттен сиретпей Kaspersky белсендіру серверлеріне сұрау жібереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Лицензия кілті клиент құрылғысынан алынған болса, оны файл түрінде экспорттау мүмкін емес.

Лицензиялық кілтті Басқару серверінің қоймасына қосу

Басқару сервері қоймасына лицензиялық кілтті қосу үшін:

1. Консоль ағашында **Kaspersky лицензиялары** қалтасын таңдаңыз.
2. Лицензиялық кілтті қосу тапсырмасын келесі тәсілдердің бірімен іске қосыңыз:
   - Лицензиялық кілттің контекстік мәзірінде **Белсендіру кодын немесе кілт файлын қосу** тармағын таңдаңыз.
   - Лицензиялық кілттер тізімін басқару блогында **Белсендіру кодын немесе кілт файлын қосу** сілтемесі арқылы өтіңіз.
   - **Белсендіру кодын немесе кілт файлын қосу** түймесін басыңыз.

   Лицензияның кілтін қосу шебері іске қосылады.
3. Басқару серверін белсендіру тәсілін таңдаңыз: белсендіру кодын пайдалану арқылы немесе кілт файлын пайдалану арқылы.
4. Белсендіру кодын немесе кілт файлын көрсетіңіз.
5. Желіңізде тиісті лицензиялық кілтті дереу таратқыңыз келсе, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін таңдаңыз. Осы параметрді таңдамасаңыз, лицензиялық кілтті кейінірек қолмен тарата аласыз.

Нәтижесінде, кілт файлы жүктеліп, Лицензияның кілтін қосу шебері аяқталады. Енді Kaspersky тізімінде осы лицензиялық кілтті көре аласыз.

Басқару серверінің лицензия кілтін өшіру

Басқару серверінің лицензия кілтін өшіру үшін:

1. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
2. Ашылған Басқару сервері сипаттары терезесінде **Лицензиялық кілттер** бөлімін таңдаңыз.
3. Лицензия кілтін **Өшіру** түймесін басу арқылы өшіріңіз.

Лицензия кілті өшіріледі.

Резервттегі лицензия кілті қосылған болса, ол алдыңғы белсенді лицензия кілті өшірілгеннен кейін автоматты түрде белсенді болады.

Басқару серверінің белсенді лицензия кілті өшірілгеннен кейін, Осалдықтар мен патчтарды басқару және Мобильдік құрылғыларды басқару функциялары қолжетімді болмайды. Өшірілген лицензия кілтін қайта қосуға немесе басқа лицензия кілтін қосуға болады.

Лицензиялық кілтті клиент құрылғыларына тарату

Kaspersky Security Center бағдарламасы *Лицензиялық кілтті тарату* тапсырмасы арқылы клиент құрылғыларына лицензиялық кілтті таратуға мүмкіндік береді.

Таратпас бұрын лицензиялық кілтті Басқару серверінің қоймасына қосыңыз.

Клиент құрылғыларына лицензиялық кілтті тарату үшін:

1. Консоль ағашында **Kaspersky лицензиялары** қалтасын таңдаңыз.
2. Лицензиялық кілттер тізімін басқару блогындағы **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** түймесін басыңыз.

   Бағдарламаны белсендіру тапсырмасын жасау шебері шеберін іске қосыңыз. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Бағдарламалар тізімінен тапсырма жасағыңыз келетін бағдарламаны таңдаңыз.
4. **Кілтті қосу** шебері қадамында келесі параметрлердің бірін пайдаланып, лицензия кілтін қосыңыз:

   - Kaspersky Security Center қоймасынан белсендіру кодын қосу үшін **Белсендіру коды** параметрін таңдаңыз.

     Таңдау түймесін басыңыз. Ашылған терезеде белсендіру кодын таңдап, **OK** түймесін басыңыз.
   - **Кілт файлы немесе кілт** параметрін таңдап, келесі әрекеттерді орындаңыз:

     a. **Таңдау** түймесін басыңыз.

     b. Контекстік мәзірден тармақтардың бірін таңдаңыз:

     - **Қалтадағы кілт файлы**.

       Құрылғыдағы ашылған терезеден кілт файлын таңдап, **Ашу** түймесін басыңыз.
     - **Kaspersky Security Center қоймасындағы кілт**.

       Ашылған терезеден Kaspersky Security Center қоймасынан кілтті таңдап, **OK** түймесін басыңыз.
5. Ағымдағы белсенді лицензия кілтін ауыстырғыңыз келсе, **Кілтті сақтық кілт ретінде пайдалану** жалаушасын алып тастаңыз.

   Мысалы, бұл ұйымыңыз өзгергенде және құрылғыда басқа ұйымның кілті қажет болғанда немесе кілт қайта шығарылған болса және ағымдағы лицензияның мерзімі біткенге дейін жаңа лицензияның мерзімі бітетін болса қажет. Қателерге жол бермеу үшін **Кілтті сақтық кілт ретінде пайдалану** жалаушасын алып тастаңыз.

   Windows жүйесіне арналған Kaspersky Security Center қолданбасына лицензия кілтін қосу кезінде туындауы мүмкін мәселелер және оларды шешу жолы туралы көбірек білгіңіз келсе, Kaspersky Security Center білім қорын қараңыз.
6. Лицензия кілті туралы ақпаратты тексеріп, **Келесі** түймесін басыңыз.

7. Шебердің осы қадамында кілт қосу тапсырмасын тағайындағыңыз келетін құрылғыларды таңдаңыз. Құрылғыларды (1000 құрылғыға дейін) келесі тәсілдердің бірімен көрсетуге болады:

   - **Басқару серверімен анықталған желілік құрылғыларды таңдау**. Құрылғылар жинағына тапсырма тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**. Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған таңдауды құрайтын құрылғыларға тағайындалады. Алдын ала анықталған таңдауды немесе өз таңдауыңызды көрсете аласыз.

   - **Басқару тобына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады.

8. Шебердің **Тапсырма кестесін конфигурациялау** қадамында тапсырманы іске қосу кестесін құрастыруға болады:

   - **Кесте бойынша іске қосу**:

     - **Бір рет**

       Тапсырма көрсетілген күн мен уақытта тек бір рет орындалады (тапсырманың жасалған күніне сәйкес).

     - **Қолмен**

       Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **Қоймаға жаңартуларды жүктеу кезінде**

       Бұл тапсырма жаңартуларды қоймаға жүктегеннен кейін іске қосылады. Мысалы, сізге осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін осы кесте қажет болуы мүмкін.

     - **Вирустық шабуылды анықтағанда**

       Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

       - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
       - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
       - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

       Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

       Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

9. Шебердің **Тапсырма атауын анықтау** қадамында тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

10. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

    Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Бағдарламаны белсендіру тапсырмасын жасау шебері шеберінің көмегімен жасалған тапсырмалар құрылғылар жинақтарына арналған тапсырмалар болып табылады және консоль ағашының **Тапсырмалар** қалтасына орналастырылады.

Сондай-ақ, басқару тобына және клиент құрылғысына тапсырма жасау шебері арқылы лицензиялық кілтті таратудың топтық немесе жергілікті тапсырмасын жасауға болады.

Лицензиялық кілтті автоматты түрде тарату

Kaspersky Security Center бағдарламасы Басқару серверіндегі кілттер қоймасында орналастырылған лицензиялық кілттерді басқарылатын құрылғыларға автоматты түрде таратуға мүмкіндік береді. Лицензиялық кілттерді автоматты түрде тарату **Тағайындалмаған құрылғылар** қалтасындағы құрылғыларға қолданылмайды.

Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату үшін

1. Консоль ағашында **Kaspersky лицензиялары** қалтасын таңдаңыз.

2. Қалтаның жұмыс аймағында құрылғыларға автоматты түрде таратқыңыз келетін лицензиялық кілтті таңдаңыз.

3. Таңдалған лицензиялық кілттің сипаттары терезесін келесі тәсілдердің бірімен ашыңыз:

   - лицензиялық кілттің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз;

   - лицензиялық кілті таңдалған жұмыс блогындағы **Лицензиялық кілттің сипаттарын көру** сілтемесі бойынша.

4. Ашылған лицензиялық кілттің сипаттары терезесінде **Автоматты түрде таратылған лицензиялық кілт** жалаушасын қойыңыз. Лицензиялық кілт сипаттары терезесін жабыңыз.

Лицензиялық кілт сай келетін құрылғыларға автоматты түрде таратылатын болады.

Лицензиялық кілтті тарату Желілік агенттің құралдарымен орындалады. Бұл арада, бағдарлама үшін резервттегі лицензиялық кілтті тарату тапсырмалары жасалмайды.

Лицензия кілтін автоматты түрде тарату кезінде құрылғылар санының лицензиялау шегі ескеріледі. (Лицензиялау шегі лицензия кілтінің сипаттарында орнатылған.) Лицензиялау шегіне жеткен болса, бұл лицензия кілтін құрылғыларға тарату автоматты түрде тоқтатылады.

Виртуалды Басқару сервері лицензиялық кілттерді өзінің қоймасынан және Басқару сервері қоймасынан автоматты түрде таратады. Ұсынылады:

- Құрылғыларға қолданғыңыз келетін лицензия кілтін таңдау үшін *Лицензия кілтін қосу* тапсырмасын пайдаланыңыз.
- Виртуалды Басқару серверінің параметрлеріндегі **Осы виртуалды Басқару серверінен өзінің құрылғыларына лицензиялық кілттерді автоматты түрде орналастыруға рұқсат беру** параметрін өшірмеңіз. Әйтпесе, виртуалды Басқару сервері лицензиялық кілттерді құрылғыларға, соның ішінде Басқару сервері қоймасынан лицензиялық кілттерді таратпайды.

Лицензиялық кілт сипаттары терезесінде **Автоматты түрде таратылған лицензиялық кілт** жалаушасын қойған болсаңыз, лицензиялық кілт сіздің желіңізде дереу таратылатын болады. Осы параметрді таңдамасаңыз, лицензиялық кілтті кейінірек қолмен тарата аласыз.

Лицензиялық кілттерді қолдану туралы есепті жасау және қарап шығу

Клиент құрылғыларында лицензиялық кілттерді пайдалану туралы есеп жасау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. **Лицензиялық кілттерді пайдалану туралы есеп** есеп үлгісін таңдаңыз немесе аттас түрдің жаңа есеп үлгісін жасаңыз.

Нәтижесінде, лицензиялық кілттерді пайдалану туралы есептің жұмыс аймағында клиент құрылғыларында қолданылатын белсенді және резервтік лицензиялық кілттер туралы ақпарат көрсетіледі. Сондай-ақ, есепте лицензиялық кілттер қолданылатын құрылғылар және лицензиялық кілттердің сипаттарында қойылған шектеулер туралы мәліметтер бар.

Бағдарламаның лицензиялық кілттері туралы ақпаратты қарап шығу

Лицензиялық кілттердің қайсысы Kaspersky бағдарламасын қолданатынын анықтау үшін:

1. Kaspersky Security Center консолі шежіресінде **Басқарылатын құрылғылар** түйінін таңдап, **Құрылғылар** қойыншасына өтіңіз.
2. Тінтуірдің оң жақ түймесімен қажетті құрылғының мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.
3. Ашылған құрылғының сипаттар терезесінде **Бағдарламалар** бөлімін таңдаңыз.
4. Пайда болған бағдарламалар тізімінен лицензиялық кілттерін көргіңіз келетін бағдарламаны таңдап, **Сипаттар** түймесін басыңыз.
5. Ашылған Басқару сервері сипаттары терезесінде **Лицензиялық кілттер** бөлімін таңдаңыз.

   Ақпарат осы бөлімнің жұмыс аймағында көрсетіледі.

Кілт файлын экспорттау

Лицензия кілті кездейсоқ жойылса және оны қалпына келтіргіңіз келсе, кілт файлын басқа Басқару серверінен экспорттауға болады.

Кілт файлын экспорттау үшін, **Жалпы функционал: Лицензия кілттерін басқару** функционалды аймағында **Кілт файлын экспорттау** құқығыңыз болуы керек.

Лицензия кілті клиент құрылғысынан алынған болса, оны экспорттау мүмкін емес.

Лицензия кілтін экспорттау үшін:

1. Консоль ағашында **Kaspersky лицензиялары** қалтасын таңдаңыз.
2. Тізімнен файл ретінде экспорттағыңыз келетін кілтті таңдаңыз.
3. Ашылған ақпараттық терезеде **Кілт файлын экспорттау** сілтемесін орындаңыз.
4. Ашылған терезеде кілт файлын сақтағыңыз келетін қалтаға жолды көрсетіңіз және файл атын көрсетіңіз. **Сақтау** түймесін басыңыз.

.key форматындағы кілт файлы таңдалған қалтаға экспортталады.

Файлы экспортталған кілт басқару серверінің қоймасына белсендіру коды ретінде қосылса және экспортталған кілт файлын басқа басқару серверінің қоймасына қосқыңыз келсе, оны кілт файлы емес, белсендіру коды ретінде қосуыңыз керек. Әйтпесе қате орын алады. Экспортталған кілт файлын ыңғайлы мәтін редакторында ашып, белсендіру кодын көшіруіңіз керек.

Желі қорғанысын конфигурациялау

Бұл бөлімде саясат пен тапсырмаларды қолмен конфигурациялау туралы, пайдаланушы рөлдері туралы, басқару топтарының құрылымын құру туралы және тапсырмалар иерархиясы туралы ақпарат бар.

Сценарий: Желі қорғанысын конфигурациялау

Бағдарламаны жылдам іске қосу шебері әдепкі бойынша параметрлері бар саясаттар мен тапсырмаларды жасайды. Бұл параметрлер ұйымда оңтайлы емес немесе тіпті тыйым салынған болуы мүмкін. Сондықтан, осы саясаттар мен тапсырмаларды конфигурациялау және сіздің желіңіз үшін қажет болса, қосымша саясаттар мен тапсырмаларды жасау ұсынылады.

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Kaspersky Security Center Басқару серверін орнаттыңыз
- Kaspersky Security Center Web Console орнаттыңыз (қажет болса)
- Kaspersky Security Center орнатудың негізгі сценарийін орындадыңыз
- Бағдарламаны жылдам іске қосу шебері аяқталды немесе келесі саясаттар мен тапсырмалар **Басқарылатын құрылғылар** басқару тобында қолмен жасалған:
  - Kaspersky Endpoint Security саясаты
  - Kaspersky Endpoint Security жаңарту топтық тапсырмасы
  - Желілік агент саясаты
  - *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы

Желі қорғанысын конфигурациялау келесі кезеңдерден тұрады:

1. **Kaspersky бағдарламалары үшін саясаттар мен саясат профильдерін конфигурациялау және тарату**

   Басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялау және тарату үшін қауіпсіздікті басқарудың екі түрлі тәсілдемесін қолдануға болады: пайдаланушыға бағытталған және құрылғыға бағытталған. Осы екі тәсілдемені біріктіруге болады. Microsoft Management Console (MMC) басқару консолі және Kaspersky Security Center Web Console негізіндегі Басқару консолі құралдары құрылғыға бағытталған қауіпсіздікті басқару әдісін іске асыруға жарамды. Пайдаланушыға бағытталған қауіпсіздікті басқарудың әдісін іске асыру үшін тек Kaspersky Security Center Web Console жарамды.

2. **Kaspersky бағдарламаларын қашықтан басқару үшін тапсырмаларды конфигурациялау**

   Бағдарламаны жылдам іске қосу шеберімен жасалған тапсырмаларды тексеріп, қажет болған жағдайда олардың параметрлерін оңтайландырыңыз.

   Нұсқаулар:

   - Басқару консолі:
     - Kaspersky Endpoint Security жаңарту топтық тапсырмасын конфигурациялау
     - Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау
   - Kaspersky Security Center Web Console:
     - Kaspersky Endpoint Security жаңарту топтық тапсырмасын конфигурациялау
     - Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері

   Қажет болса, клиент құрылғыларында орнатылған Kaspersky бағдарламаларын басқарудың қосымша тапсырмаларын жасаңыз.

3. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

Басқарылатын қолданбалар жұмысы кезінде пайда болатын оқиғалар туралы ақпарат клиент құрылғысынан тасымалданады және басқару серверінің дерекқорына тіркеледі. Басқару серверіне түсетін жүктемені азайту үшін дерекқорда сақталуы мүмкін оқиғалардың ең көп санын бағалаңыз және шектеңіз.

Нұсқаулар:

- Басқару консолі: Оқиғалардың ең көп санын конфигурациялау
- Kaspersky Security Center Web Console: Оқиғалардың ең көп санын конфигурациялау

Нәтижелер

Осы сценарий аяқталғаннан кейін, сіздің желіңіз Kaspersky бағдарламаларын, Басқару сервері алатын тапсырмалар мен оқиғаларды конфигурациялау арқылы қорғалады:

- Kaspersky бағдарламалары саясаттар мен саясат профильдеріне сай конфигурацияланған.
- Бағдарламаларды басқару тапсырмалар жиынтығының көмегімен жүзеге асырылады.
- Дерекқорда сақталуы мүмкін оқиғалардың ең көп саны белгіленген.

Желі қорғанысын конфигурациялап болғаннан кейін, сіз Kaspersky дерекқорлары мен қолданбаларына арналған тұрақты жаңартуларды конфигурациялауға өте аласыз.

Kaspersky Sandbox-та анықталған қауіптерге автоматты түрде жауап беруді конфигурациялау туралы толық ақпаратты Kaspersky Sandbox 2.0 онлайн анықтамасынан қараңыз.

Саясаттарды конфигурациялау және тарату: құрылғыларға бағытталған тәсілдеме

Осы сценарий аяқталғаннан кейін, қолданбалар сіз анықтайтын қолданба саясаттары мен саясат профильдеріне сәйкес барлық басқарылатын құрылғыларда конфигурацияланады.

Алдын ала талаптар

Kaspersky Security Center Басқару серверін және Kaspersky Security Center Web Console веб-консолін (қажет болса) орнатқаныңызға көз жеткізіңіз. Kaspersky Security Center Web Console орнатқан болсаңыз, сізді құрылғыға бағытталған қауіпсіздікті басқаруға балама немесе қосымша ретінде пайдаланушыға бағдарланған қауіпсіздікті басқару да қызықтыруы мүмкін.

Кезеңдер

Құрылғыларға бағытталған Kaspersky бағдарламаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Бағдарламалар саясаттарын конфигурациялау**

Әр бағдарлама үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялаңыз. Бұл саясат жиынтығы клиент құрылғыларына қолданылады.

Бағдарламаны жылдам іске қосу шебері арқылы желі қорғанысын конфигурациялау кезінде Kaspersky Security Center бағдарламасы келесі бағдарламалар үшін әдепкі бойынша саясатты жасайды:

- Kaspersky Endpoint Security for Windows – Windows операциялық жүйесі бар клиент құрылғылары үшін
- Kaspersky Endpoint Security for Linux – Linux операциялық жүйесі бар клиент құрылғылары үшін

Егер сіз осы шебердің көмегімен конфигурациялау процесін аяқтаған болсаңыз, сізге бұл бағдарлама үшін жаңа саясат жасаудың қажеті жоқ. Kaspersky Endpoint Security саясатын қолмен конфигурациялауға өтіңіз.

Егер сізде бірнеше Басқару серверінің және/немесе басқару топтарының иерархиялық құрылымы болса, қосалқы Басқару серверлері мен еншілес басқару топтары саясатты әдепкі бойынша негізгі Басқару серверінен иеленеді. Саясат параметрлерін иерархия бойынша төмен қарай өзгертуге тыйым салу үшін параметрлерді еншілес топтар мен қосалқы Басқару серверлеріне мәжбүрлеп иелендіруге болады. Егер сіз параметрлердің тек бір бөлігін иеленуге рұқсат бергіңіз келсе, оларды саясат иерархиясы бойынша жоғары деңгейде құлыптай аласыз. Басқа құлыпталмаған параметрлер иерархия бойынша төменгі саясатты өзгерту үшін қолжетімді болады. Құрылған саясат иерархиясы басқару топтарындағы құрылғыларды тиімді басқаруға мүмкіндік береді.

Нұсқаулар:

- Басқару консолі: Саясат жасау
- Kaspersky Security Center Web Console: саясат жасау

2 Саясат профильдерін жасау (қажет болса)

Егер сіз бір басқару тобындағы құрылғыларға әртүрлі саясат параметрлерін қолданғыңыз келсе, сол құрылғылар үшін саясат профильдерін жасаңыз. Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер басқарылатын құрылғыда әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды.

Профильді белсендіру шарттарын қолдана отырып, сіз әртүрлі саясат профильдерін қолдана аласыз, мысалы, белгілі бір бөлімшеде немесе Active Directory қауіпсіздік тобында орналасқан, белгілі бір бағдарламалық жасақтама конфигурациясы бар немесе белгіленген тегтері бар құрылғыларға. Белгілі бір өлшемшарттарға сәйкес келетін құрылғыларды сүзгілеу үшін тегтерді пайдаланыңыз. Мысалы, сіз *Windows* тегін жасай аласыз, оны Windows операциялық жүйесі басқаратын барлық құрылғыларға тағайындай аласыз, содан кейін бұл тегті саясат профилін белсендіру ережелерінде көрсете аласыз. Нәтижесінде, Windows операциялық жүйесі басқаратын құрылғыларда орнатылған Kaspersky бағдарламалары өздерінің саясат профилімен басқарылатын болады.

Нұсқаулар:

- Басқару консолі:
  - Саясат профилін жасау
  - Саясатын профилін белсендіру ережесін жасау
- Kaspersky Security Center Web Console:
  - Саясат профилін жасау
  - Саясатын профилін белсендіру ережесін жасау

3 Саясаттар мен саясат профильдерін басқарылатын құрылғыларға тарату

Әдепкі бойынша, басқарылатын құрылғыларды Басқару серверімен синхрондау 15 минут сайын бір рет жүзеге асырылады. Автоматты синхрондауды өткізіп жіберіп, синхрондауды Мәжбүрлеп синхрондау пәрмені арқылы қолмен іске қосуға болады. Сондай-ақ, мәжбүрлеп синхрондау саясатты немесе саясат профилін жасағаннан немесе өзгерткеннен кейін орындалады. Синхрондау кезінде басқарылатын құрылғыларға жаңа немесе өзгертілген саясат пен саясат профильдері қолданылады.

Kaspersky Security Center Web Console қолдансаңыз, саясат пен саясат профильдерінің құрылғыларға жеткізілгенін тексеруге болады. Kaspersky Security Center бағдарламасы құрылғының сипаттарында жеткізу күні мен уақытын анықтайды.

Нұсқаулар:

- Басқару консолі: Мәжбүрлеп синхрондау
- Kaspersky Security Center Web Console: Мәжбүрлеп синхрондау

Нәтижелер

Құрылғыларға бағытталған сценарий аяқталғаннан кейін, Kaspersky бағдарламалары саясат иерархиясы арқылы көрсетілген және таралған параметрлерге сәйкес конфигурацияланады.

Бағдарлама саясаттары мен саясат профильдері басқару топтарына қосылған жаңа құрылғыларға автоматты түрде қолданылады.

Құрылғыларға және пайдаланушыларға бағытталған қауіпсіздікті басқару тәсілдемелері

Қауіпсіздік параметрлерін құрылғының функциялары мен пайдаланушы рөлдері жайғасымынан басқаруға болады. Бірінші тәсілдемесі *құрылғыларға бағытталған қауіпсіздікті басқару*, екіншісі тәсілдемесі *пайдаланушыларға бағытталған қауіпсіздікті басқару* деп аталады. Бағдарламалардың әртүрлі параметрлерін әртүрлі құрылғыларға қолдану үшін, сіз тіркесімдегі бір немесе екі басқару түрін қолдана аласыз. Microsoft Management Console (MMC) басқару консолі және Kaspersky Security Center Web Console негізіндегі Басқару консолі құралдары құрылғыға бағытталған қауіпсіздікті басқару әдісін іске асыруға жарамды. Пайдаланушыға бағытталған қауіпсіздікті басқарудың әдісін іске асыру үшін тек Kaspersky Security Center Web Console жарамды.

Құрылғыға бағытталған қауіпсіздікті басқару құрылғының ерекшеліктеріне байланысты басқарылатын құрылғыларға қауіпсіздік бағдарламасының әртүрлі параметрлерін қолдануға мүмкіндік береді. Мысалы, әртүрлі басқару топтарында орналасқан құрылғыларға әртүрлі параметрлерді қолдануға болады. Сондай-ақ, құрылғыларды Active Directory-де немесе аппараттық жасақтаманың сипаттамалары бойынша пайдалану арқылы ажыратуға болады.

Пайдаланушыға бағытталған қауіпсіздікті басқару қауіпсіздік бағдарламаларының әртүрлі параметрлерін әртүрлі пайдаланушы рөлдеріне қолдануға мүмкіндік береді. Сіз бірнеше пайдаланушы рөлдерін жасай аласыз, әр пайдаланушыға сәйкес келетін пайдаланушы рөлін тағайындай аласыз және әртүрлі рөлдері бар пайдаланушыларға тиесілі құрылғылар үшін әртүрлі бағдарлама параметрлерін анықтай аласыз. Мысалы, бағдарламалардың әртүрлі параметрлерін бухгалтерлердің құрылғыларына және кадрлар бөлімі мамандарының құрылғыларына қатысты қолдануға болады. Пайдаланушыларға бағытталған қауіпсіздікті басқаруды енгізу нәтижесінде, әрбір бөлім – бухгалтерия бөлімі мен кадрлар бөлімі – Kaspersky бағдарламаларымен жұмыс істеуге арналған параметрлердің өзіндік конфигурациясын алады. Параметрлер конфигурациясы бағдарламаның қандай параметрлерін пайдаланушылар өзгерте алатынын, ал қайсысын әкімші мәжбүрлеп орнатып, бұғаттай алатынын анықтайды.

Пайдаланушыларға бағытталған қауіпсіздікті басқару жекелеген пайдаланушылар үшін белгіленген бағдарлама параметрлерін қолдануға мүмкіндік береді. Бұл, қызметкерге ұйымда бірегей рөл тағайындалса немесе белгілі бір қызметкерге қатысты қауіпсіздік мәселелерін бақылау керек болса, қажет болуы мүмкін. Бұл қызметкердің компаниядағы рөліне байланысты, бағдарламаның параметрлерін өзгерту үшін, оның құқықтарын кеңейтуге немесе қысқартуға болады. Мысалы, жергілікті кеңседе клиент құрылғыларын басқаратын жүйелік әкімшінің құқықтарын кеңейту қажет болуы мүмкін.

Сондай-ақ, сіз пайдаланушыларға бағытталған және құрылғыларға бағытталған қауіпсіздікті басқару тәсілдемелерін біріктіре аласыз. Мысалы, әрбір басқару тобы үшін әртүрлі саясаттарды конфигурациялауға, содан кейін ұйымыңыздың бір немесе бірнеше пайдаланушы рөлі үшін саясат профильдерін қосымша түрде жасауға болады. Бұл жағдайда, саясаттар мен саясат профильдері келесі тәртіпте қолданылады:

1. Құрылғыларға бағытталған қауіпсіздікті басқару үшін жасалған саясаттар қолданылады.
2. Олар саясат профильдерінің параметрлеріне сәйкес саясат профильдерімен түрлендіріледі.
3. Саясаттар пайдаланушы рөлдерімен байланысты саясат профильдерімен түрлендіріледі.

Kaspersky Endpoint Security саясатын қолмен конфигурациялау

Осы бөлім Бағдарламаны жылдам іске қосу шебері жасайтын Kaspersky Endpoint Security саясатының параметрлерін конфигурациялау бойынша ұсынымдарды қамтиды. Саясат сипаттары терезесінде конфигурациялауды орындауға болады.

Параметрді өңдеген кезде, оның мәнін жұмыс станциясында пайдалану үшін тиісті параметрдің үстіңгі жағындағы құлып белгішесін басуыңыз керек.

Кеңейтілген қорғаныс бөлімінде саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Кеңейтілген қорғаныс бөлімінде Kaspersky Endpoint Security for Windows үшін Kaspersky Security Network қолданысын конфигурациялауға болады. Сондай-ақ, Әрекеттерді талдау, Эксплойттан қорғаныс, Хост-компьютерге басып кіруді болдырмау және Зиянды әрекеттерді шегіндіру сияқты Kaspersky Endpoint Security for Windows модульдерін конфигурациялауға болады.

Kaspersky Security Network ішкі бөлімінде **Kaspersky Security Network** опциясын қосуға кеңес беріледі. Бұл параметрді пайдалану желі трафигін қайта таратуға және оңтайландыруға көмектеседі. **Kaspersky Security Network** опциясы өшірілсе, KSN серверлерін тікелей пайдалануды қосуға болады.

Негізгі қорғаныс бөліміндегі саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Саясат сипаттары терезесінің **Негізгі қорғаныс** бөлімінде **Желілік экран** және **Файл қауіптерінен қорғаныс** ішкі бөлімдерінде қосымша параметрлерді көрсету ұсынылады.

Желілік экран ішкі бөлімі клиент құрылғыларында қолданбалардың желілік әрекетін бақылауға көмектесетін параметрлерді қамтиды. Клиент құрылғысы келесі күйлердің бірі берілген желіні пайдаланады: жалпыға қолжетімді, жергілікті немесе сенімді. Желі күйіне байланысты Kaspersky Endpoint Security құрылғыдағы желілік белсенділікке рұқсат етуі немесе тыйым салуы мүмкін. Ұйымыңызға жаңа желіні қосқан кезде, оған сәйкес желілік күйді беруіңіз керек. Мысалы, егер ноутбук клиент құрылғысы болса, бұл құрылғы жалпыға қолжетімді немесе сенімді желіні пайдалануы ұсынылады, өйткені ноутбук әрқашан жергілікті желіге қосылған болмайды. **Желілік экран** ішкі бөлімінде ұйымда қолданылатын желілерге күйлерді дұрыс тағайындағаныңызды тексеруге болады.

Желілер тізімін тексеру үшін:

1. Саясат сипаттарында **Негізгі қорғаныс** → **Желілік экран** бөліміне өтіңіз.
2. **Қолжетімді желілер** бөлімінде **Параметрлер** түймесін басыңыз.
3. Ашылған **Желілік экран** терезесінде желілер тізімін көру үшін **Желі** қойындысына өтіңіз.

Файл қауіптерінен қорғаныс ішкі бөлімінде желі дискілерін сканерлеуді өшіруге болады. Желілік дисктерді тексеру желілік дисктерге айтарлықтай жүктемені тудыра алады. Тікелей файл серверлерінде тексеруді жүзеге асырған жөн.

Желілік дискіні тексеруді өшіру үшін:

1. Саясат сипаттарында **Негізгі қорғаныс** → **Файл қауіптерінен қорғаныс** бөліміне өтіңіз.
2. **Қауіпсіздік деңгейі** бөлімінде **Параметрлер** түймесін басыңыз.
3. Ашылған **Файл қауіптерінен қорғаныс** терезесіндегі **Жалпы** қойындысында **Барлық желілік дискілер** құсбелгі ұяшығын тазалаңыз.

Қосымша параметрлер бөліміндегі саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Саясат сипаттары терезесінің **Жалпы параметрлер** бөлімінде **Есептер және қойма** және **Интерфейс** ішкі бөлімдерінде қосымша параметрлерді көрсету ұсынылады.

Есептер және қойма ішкі бөлімінде **Деректерді басқару серверіне тасымалдау** бөліміне өтіңіз. **Іске қосылатын бағдарламалар туралы** құсбелгі ұяшығы басқару серверінің дерекқорында желі құрылғыларында барлық бағдарламалық жасақтама модулінің барлық нұсқасы туралы ақпарат сақтала ма екендігін көрсетеді. Егер бұл жалауша орнатылса, сақталған ақпарат Kaspersky Security Center дерекқорында айтарлықтай көлемді алуы мүмкін (ондаған гигабайт). **Іске қосылатын бағдарламалар туралы** құсбелгі ұяшығы жоғары деңгейлі саясатта таңдалған болса, оны тазалаңыз.

Басқару консолі ұйымның желісінде қорғанысты орталықтандырылған түрде басқарса, жұмыс станцияларында Kaspersky Endpoint Security for Windows пайдаланушы интерфейсін көрсетуді өшіріңіз. Ол үшін **Интерфейс** ішкі бөлімінде **Пайдаланушымен өзара әрекеттесу** бөліміне өтіп, **Пайдаланушы интерфейсін көрсетпеу** опциясын таңдаңыз.

Жұмыс станцияларында құпиясөзбен қорғанысты қосу үшін **Интерфейс** ішкі бөлімінде **Құпиясөзбен қорғау** бөліміне өтіңіз, **Параметрлер** түймесін басып, **Құпиясөзбен қорғауды қосу** құсбелгі ұяшығын таңдаңыз.

Оқиғаларды конфигурациялау бөліміндегі саясатты конфигурациялау

Оқиғаларды конфигурациялау бөлімінде төменде аталған оқиғалардан басқа барлық оқиғаны басқару серверінде сақтауды өшіру керек:

- **Критикалық** қойындысында:
  - *Бағдарламаны автоматты түрде іске қосу өшірілді*
  - *Қатынасуға тыйым салынған*
  - *Бағдарламаны іске қосуға рұқсат берілмеген*
  - *Емдеу мүмкін емес*
  - *Түпкі пайдаланушының лицензиялық келісімі бұзылды*
  - *Шифрлау модулін жүктеу мүмкін болмады*
  - *Екі тапсырманы бір уақытта іске қосу мүмкін емес*
  - *Белсенді қауіп анықталды. Белсенді зақымдауды емдеу процедурасын іске қосу керек*
  - *Желілік шабуыл анықталды*
  - *Барлық компоненттер жаңартылмады*
  - *Белсендіру қатесі*
  - *Ықшам режимді белсендіру қатесі*
  - *Kaspersky Security Center орталығымен өзара әрекеттесу қатесі*
  - *Портативті режимді өшіру қатесі*
  - *Бағдарлама компоненттерінің құрамын өзгерту қатесі*
  - *Файлдарды шифрлау/шифрын шешу ережелерін қолдану қатесі*

- *Саясатты қолдану мүмкін емес*
- *Процесс аяқталды*
- *Желілік белсенділікке рұқсат берілмеген*

- **Функционалдық ақау** қойындысында: *Тапсырма параметрлеріндегі қате. Тапсырма параметрлері қолданылмады*
- **Ескерту** қойындысында:
  - *Бағдарламаның өзіндік қорғанысы өшірілді*
  - *Резервті кілті дұрыс емес*
  - *Пайдаланушы шифрлау саясатынан бас тартты*
- **Ақпараттық** қойындысында: *Бағдарламаны сынақ режимде іске қосуға тыйым салынған*

Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау

10 және одан жоғары нұсқадағы Kaspersky Endpoint Security үшін оңтайлы және ұсынылатын кесте нұсқасы – **Қоймаға жаңартуларды жүктеу кезінде** жалауша орнатылған кезде **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**.

Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері құрылғыны тексерудің топтық тапсырмасын жасайды. Әдепкі бойынша тапсырма үшін автоматты рандомизациясы бар **Жұма күндері 19:00-де іске қосу** кестесі таңдалды және **Өткізіп алынған тапсырмаларды іске қосу** жалаушасы алынды.

Демек, егер ұйымның құрылғылары жұма күндері сағат 18:30-да сөндірілсе, онда құрылғыны сканерлеу тапсырмасы ешқашан іске қосылмайды. Ұйымда қабылданған жұмыс регламентіне сүйене отырып осы тапсырманың оңтайлы кестесін конфигурациялау керек.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау

Бағдарламаны жылдам іске қосу шебері Желілік агент үшін *Осалдықтарды және қажетті жаңартуларды іздеу* топтық тапсырмасын жасайды. Әдепкі бойынша тапсырма үшін автоматты рандомизациясы бар **Сейсенбі күндері 19:00-де іске қосу** кестесі таңдалды және **Өткізіп алған тапсырмаларды іске қосу** жалаушасы орнатылды.

Егер ұйым жұмысының регламенті осы уақытта құрылғыларды сөндіруді қарастырса, онда *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыны қосқаннан кейін (сәрсенбі күні таңертең) іске қосылады. Мұнда жүріс-тұрыс жағымсыз болуы мүмкін, өйткені осалдықтарды іздеу құрылғының процессоры мен диск ішкі жүйесіне жоғары жүктеме түсіруі мүмкін. Ұйымда қабылданған жұмыс регламентіне сүйене отырып, тапсырманың оңтайлы кестесін конфигурациялау керек.

Жаңартуларды орнату және осалдықты түзету топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері Желілік агент үшін жаңартуларды орнату және осалдықтарды іздеу топтық тапсырмасын жасайды. Әдепкі бойынша автоматты түрде рандомизациясы бар күн сайын 1:00-де тапсырманы іске қосу конфигурацияланған, **Өткізіп алынған тапсырмаларды іске қосу** параметрі сөндірілген.

Егер ұйымның жұмыс регламенті құрылғыны түнде сөндіруді қарастырса, онда жаңартуларды орнату тапсырмасы ешқашан іске қосылмайды. Ұйымда қабылданған жұмыс регламентіне сүйеніп, осалдықтарды іздеу тапсырмасының оңтайлы кестесін белгілеу керек. Сонымен қатар, жаңартуларды орнату нәтижесінде құрылғыны қайта іске қосу қажет болуы мүмкін екендігін ескерген жөн.

Оқиғалар қоймасындағы оқиғалар санын конфигурациялау

Басқару сервері сипаттары терезесінің **Оқиғалар қоймасы** бөлімінде Басқару серверінің дерекқорында оқиғаларды сақтау параметрлерін конфигурациялауға болады: оқиғалар туралы жазбалар санын және жазбаларды сақтау уақытын шектеу. Оқиғалардың ең көп санын көрсеткенде, бағдарламалар оқиғалардың көрсетілген санын сақтау үшін диск кеңістігінің долбарлы өлшемін есептейді. Сіз бұл есептеуді дерекқордың толып кетуіне жол бермеу үшін бос диск кеңістігінің жеткілікті ме екенін бағалау үшін пайдалана аласыз. Әдепкі бойынша, Басқару сервері дерекқорының сыйымдылығы 400 000 оқиғаны құрайды. Дерекқордың ұсынылған ең жоғары сыйымдылығы 45 000 000 оқиғаны құрайды.

Бағдарлама дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, бағдарлама оқиғалардың көрсетілген ең көп саны ғана қалуы үшін ең ескі оқиғаларды жояды.

Басқару сервері ескі оқиғаларды жойған кезде, ол жаңа оқиғаларды дерекқорға сақтай алмайды. Осы кезең ішінде қабылданбаған оқиғалар туралы ақпарат Kaspersky Event журналына жазылады. Жаңа оқиғалар кезекке қойылады, содан соң жою операциясы аяқталғаннан кейін, дерекқорда сақталады.

Басқару серверіндегі оқиғалар қоймасында сақтауға болатын оқиғалар санын шектеу үшін:

1. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Оқиғалар қоймасы** бөлімінде, дерекқорда сақталатын оқиғалардың максималды санын көрсетіңіз.

3. **ОК** түймесін басыңыз.

Тапсырманы орындау барысына қатысты оқиғаларды сақтау немесе тек тапсырманы орындау нәтижелерін сақтау үшін кез келген тапсырманың параметрлерін өзгертуге де болады. Осылайша, сіз дерекқордағы оқиғалардың санын азайтасыз, дерекқордағы оқиғалар кестесін талдаумен байланысты сценарийлердің жұмыс жылдамдығын арттырасыз және критикалық оқиғаларды оқиғалардың көп санымен ығыстыру қаупін азайтасыз.

Түзетілген осалдықтар туралы ақпаратты сақтаудың максималды мерзімін белгілеу

Басқарылатын құрылғылардағы түзетілген осалдықтар туралы ақпаратты дерекқорда сақтаудың ең көп мерзімін белгілеу үшін:

1. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Оқиғалар қоймасы** бөлімінде, дерекқордағы түзетілген осалдықтар туралы ақпаратты сақтаудың ең көп мерзімін көрсетіңіз.

   Әдепкі бойынша белгіленген мерзім – 90 күн.

3. **ОК** түймесін басыңыз.

Түзетілген осалдықтар туралы ақпаратты сақтаудың ең көп мерзімі көрсетілген күндер санымен шектеледі. Осыдан кейін, Басқару серверіне қызмет көрсету тапсырмасы дерекқордан ескірген ақпаратты жояды.

Тапсырмаларды басқару

Kaspersky Security Center түрлі тапсырмаларды құру және іске қосу арқылы құрылғыларда орнатылған бағдарламалардың жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Тапсырмалар келесі түрлерге бөлінеді:

- *Топтық тапсырмалар*. Таңдалған басқару тобының құрылғыларында орындалатын тапсырмалар.
- *Басқару серверінің тапсырмалары*. Басқару серверінде орындалатын тапсырмалар.
- *Арнайы құрылғыларға арналған тапсырмалар*. Глобалдық тапсырмалар – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.
- *Жергілікті тапсырмалар*. Жергілікті тапсырмалар – нақты құрылғыда орындалатын тапсырмалар.

Бағдарлама үшін тапсырмаларды құру, тек осы бағдарламаны басқару плагині әкімшінің жұмыс станциясына орнатылған жағдайда ғана мүмкін болады.

Тапсырма (1000 құрылғыға дейін) жасалатын құрылғылардың тізімін келесі тәсілдердің бірімен жасауға болады:

- Басқару серверімен анықталған желілік құрылғыларды таңдау.
- Құрылғылар тізімін қолмен белгілеу. Құрылғының мекенжайы ретінде сіз IP мекенжайын (немесе IP аралығын), NetBIOS немесе DNS атауын пайдалана аласыз.

- Құрылғылар тізімін қосылатын құрылғылар мекенжайлары тізбесін қамтитын TXT пішіміндегі файлдан құрылғылар тізімін импорттау (әр мекенжай бөлек жолда орналасуы тиіс).

  Егер құрылғылар тізімі файлдан импортталса немесе қолмен қалыптастырылса, ал құрылғылар атауы бойынша анықталса, онда құрылғыларды қосу кезінде немесе құрылғыларды табу нәтижесінде тізімге ақпараты Басқару серверінің дерекқорына әлдеқашан қосылған құрылғылар ғана қосылуы мүмкін.

Әр бағдарлама үшін сіз топтық тапсырмалардың, арнайы құрылғыларға арналған тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Құрылғыда орнатылған бағдарлама мен Kaspersky Security Center ақпараттық дерекқоры арасындағы тапсырмалар туралы ақпарат алмасу Желілік агент Басқару серверіне қосылған сәтте орын алады.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Тапсырма жасалған қолданба жұмыс істеп тұрса ғана, тапсырмалар құрылғыда іске қосылады. Бағдарлама тоқтаған кезде барлық іске қосылған тапсырмалардың орындалуы тоқтатылады.

Тапсырмаларды орындау нәтижелері Microsoft Windows оқиғалар журналдарында және Kaspersky Security Center орталықтандырылған Басқару серверінде де, әр құрылғыда да сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Көптиістілікті қолдайтын бағдарламалар үшін тапсырмаларды басқару

Көптиістілікті бағдарламаларға арналған топтық тапсырма Басқару серверлері мен клиент құрылғыларының иерархиясына байланысты бағдарламаларға қолданылады. Тапсырма жасалған виртуалды Басқару сервері бағдарлама орнатылған клиент құрылғысымен немесе төменгі деңгейдегі топпен бірдей Басқару тобында болуы керек.

Тапсырманы орындау нәтижелеріне сәйкес келетін оқиғаларда провайдердің әкімшісі тапсырма орындалған құрылғы туралы ақпаратты көрсетеді. Өз кезегінде, клиент әкімшісіне **Көп пайдаланушылық түйін** көрсетіледі.

Тапсырманы жасау

Басқару консолінде тапсырманы тікелей тапсырма жасалатын басқару тобының қалтасында және **Тапсырмалар** қалтасының жұмыс аймағында жасауға болады.

Басқару топтары қалтасында топтық тапсырманы жасау үшін:

1. Консоль ағашында тапсырманы жасау үшін басқару тобын таңдаңыз.
2. Жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.
3. **Тапсырма жасау** түймесі бойынша тапсырманы жасау шеберін іске қосыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

***Тапсырмалар** қалтасының жұмыс аймағында тапсырманы жасау үшін:*

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Аяқтау** түймесі бойынша тапсырманы жасау шеберін іске қосыңыз.

Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Басқару серверінің тапсырмасын жасау

Басқару сервері келесі функцияларды орындайды:

- Есептерді жеткізу
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу
- Басқару сервері деректерін сақтық көшірмелеу
- Басқару серверіне техникалық қызмет көрсету
- Windows Update жаңартуларын синхрондауды орындау
- Анықтамалық құрылғының ОЖ кескінінің орнату пакетін жасау
- Бағдарламаларды қашықтан орнату
- Бағдарламаларды қашықтан жою
- Орнату пакеттерін тарату
- Қолданбаны қосымша басқару серверлеріне қашықтан орнату

Виртуалды Басқару серверінде есептерді автоматты түрде жеткізу және анықтамалық құрылғының операциялық жүйесінің кескініне негізделген орнату пакетін жасау тапсырмасы ғана қолжетімді. Виртуалды сервердің қоймасы негізгі Басқару серверіне жүктелген жаңартуларды көрсетеді. Виртуалды сервер деректерінің сақтық көшірмесі негізгі Басқару сервері деректерінің сақтық көшірмесі шеңберінде жүзеге асырылады.

Басқару серверінің тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. Жасау процесін келесі тәсілдердің бірімен іске қосыңыз:
   - Консоль тармағындағы **Тапсырмалар** қалтасының контекстік мәзіріндегі **Жаңа** → **Тапсырма** тармағын таңдау арқылы.
   - **Тапсырма жасау** қалтасының жұмыс аймағында **Тапсырмалар** түймесін басыңыз.

Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу, Windows Update жаңартуларын синхрондау, Басқару серверіне қызмет көрсету және *Басқару сервері деректерінің резервтік қоймасы* тапсырмаларын бір үлгіде ғана жасауға болады. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*, *Басқару серверіне қызмет көрсету*, *Басқару сервері деректерінің резервтік қоймасы* және *Windows Update жаңартуларын синхрондау* тапсырмалары Басқару сервері үшін әлдеқашан жасалып қойған болса, олар жаңа тапсырма жасау шебері тапсырмасы түрін таңдау терезесінде көрсетілмейді.

Арнайы құрылғыларға арналған тапсырмалар жасау

Kaspersky Security Center бағдарламасында сіз кездейсоқ таңдалған құрылғылар жиынтығына тапсырмалар жасай аласыз. Жиынтықтағы құрылғылар әртүрлі басқару топтарына кіруі немесе кез келген басқару тобына кірмеуі мүмкін. Kaspersky Security Center бағдарламасы құрылғылар жиынтығы үшін келесі негізгі тапсырмаларды орындауға мүмкіндік береді:

- Бағдарламаларды қашықтан орнату
- Пайдаланушыға хабар жіберу
- Басқару серверін ауыстыру
- Құрылғыларды басқару
- Жаңартуды тексеру
- Орнату пакеттерін тарату
- Қолданбаны қосымша басқару серверлеріне қашықтан орнату
- Бағдарламаларды қашықтан жою

Арнайы құрылғыларға арналған тапсырмалар жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. Жасау процесін келесі тәсілдердің бірімен іске қосыңыз:
   - Консоль тармағындағы **Тапсырмалар** қалтасының контекстік мәзіріндегі Тапсырма → **Тапсырмалар** тармағын таңдау арқылы.
   - **Тапсырма жасау** қалтасының жұмыс аймағында **Тапсырмалар** түймесін басыңыз.

Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Жергілікті тапсырма жасау

Құрылғыға жергілікті тапсырма жасау үшін:

1. Құрылғы кіретін топтың жұмыс аймағында **Құрылғылар** қойыншасын таңдаңыз.
2. **Құрылғылар** қойыншасындағы құрылғылар тізімінен жергілікті тапсырма жасау керек құрылғыны таңдаңыз.
3. Келесі тәсілдердің бірімен таңдалған құрылғы үшін тапсырма жасау процесін бастаңыз:
   - **Әрекетті орындау** түймесін басыңыз да, ашылатын тізімнен **Тапсырма жасау** мәнін таңдаңыз.
   - Құрылғының жұмыс аймағында **Тапсырма жасау** сілтемесінен өтіңіз
   - Құрылғының сипаттарын келесідей қолданыңыз:
     a. Құрылғының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.
     b. Құрылғының ашылған сипаттар терезесінде **Тапсырмалар** бөлімін таңдап, **Қосылуда** түймесін басыңыз.

Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Жергілікті тапсырмаларды жасау мен конфигурациялаудың егжей-тегжейлі сипаттамалары Kaspersky тиісті бағдарламаларына арналған нұсқаулықтарда келтірілген.

Салынған топтың жұмыс аймағында иеленген топтық тапсырманы көрсету

Жұмыс аймағында салынған топтың иеленген тапсырмаларын көрсетуді қосу үшін:

1. Салынған топтың жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.
2. **Тапсырмалар** қойыншасының жұмыс аймағында **Иеленген тапсырмаларды көрсету** түймесін басыңыз.

Нәтижесінде, иеленген тапсырмалар келесі белгішесі бар тапсырма тізімінде көрсетіледі:

-  – егер олар негізгі Басқару серверінде құрылған топтан иеленген болса;
-  – егер олар жоғарғы деңгейдегі топтан иеленген болса.

Иелену режимі қосылған кезде, иеленген тапсырмаларды өңдеу олар құрылған топта ғана қолжетімді. Иеленген тапсырмаларды өңдеу тапсырманы иеленетін топта қолжетімді емес.

Тапсырманы іске қоспас бұрын құрылғыларды автоматты түрде қосу

Kaspersky Security Center бағдарламасы өшірулі құрылғыларда тапсырмаларды орындамайды. Сіз Kaspersky Security Center бағдарламасын Wake-on-LAN функциясының көмегімен тапсырманы іске қоспас бұрын осы құрылғыларды автоматты түрде қосатындай етіп конфигурациялай аласыз.

Тапсырманы іске қоспас бұрын құрылғылардың автоматты түрде қосылуын конфигурациялау үшін:

1. Тапсырма сипаттары терезесінде **Кесте** бөлімін таңдаңыз.
2. Құрылғылардағы әрекеттерді конфигурациялау үшін **Кеңейтілген** сілтемесіне өтіңіз.
3. Ашылған **Кеңейтілген** терезесінде **Тапсырманы бастамас бұрын, Желі арқылы қашықтан қосу технологиясы арқылы құрылғыларды іске қосу (мин)** жалаушасын қойып, минуттағы уақытты көрсетіңіз.

Нәтижесінде, тапсырманы іске қосудан бірнеше минут бұрын, Kaspersky Security Center бағдарламасы құрылғыларды қосады және операциялық жүйені Wake-on-LAN функциясы арқылы жүктейді. Тапсырманы орындағаннан кейін, құрылғы пайдаланушылары жүйеге кірмесе, құрылғылар автоматты түрде өшеді. Kaspersky Security Center бағдарламасы тек Wake-on-LAN функциясы арқылы қосылған құрылғыларды автоматты түрде өшіреді.

Kaspersky Security Center бағдарламасы операциялық жүйелерді тек Wake-on-LAN (WoL) стандартын қолдайтын құрылғыларда автоматты түрде іске қоса алады.

Тапсырманы орындағаннан кейін құрылғыны автоматты түрде өшіру

Kaspersky Security Center бағдарламасы тапсырма параметрлерін орындағаннан кейін, ол таратылатын құрылғылар автоматты түрде өшірілетіндей етіп конфигурациялауға мүмкіндік береді.

Тапсырманы орындағаннан кейін құрылғыларды автоматты түрде өшіру үшін:

1. Тапсырма сипаттары терезесінде **Кесте** бөлімін таңдаңыз.
2. **Кеңейтілген** сілтемесі арқылы құрылғылармен жасалатын әрекеттерді конфигурациялау терезесін ашыңыз.
3. Ашылған **Кеңейтілген** терезесінде **Тапсырманы орындағаннан кейін құрылғыларды өшіру** жалаушасын қойыңыз.

Тапсырманы орындау уақытын шектеу

Құрылғылардағы тапсырманың орындалу уақытын шектеу үшін:

1. Тапсырма сипаттары терезесінде **Кесте** бөлімін таңдаңыз.
2. **Кеңейтілген** сілтемесі арқылы клиент құрылғыларымен жасалатын әрекеттерді конфигурациялау терезесін ашыңыз.
3. Ашылған **Кеңейтілген** терезесінде **Тапсырма мынанша минуттан көбірек орындалып жатса, оны тоқтату (мин)** жалаушасын қойып, минуттағы уақытты көрсетіңіз.

Нәтижесінде, егер көрсетілген уақыттан кейін құрылғыдағы тапсырманы орындау аяқталмаса, Kaspersky Security Center бағдарламасы тапсырманы автоматты түрде тоқтатады.

Тапсырманы экспорттау

Сіз топтық тапсырмаларды және арнайы құрылғыларға арналған тапсырмаларды файлға экспорттай аласыз. Басқару серверінің тапсырмалары да экспорттау үшін қолжетімді емес.

Тапсырманы экспорттау үшін:

1. Тапсырманың мәнмәтіндік мәзірінде **Барлық тапсырмалар** → **Экспорттау** тармағын таңдаңыз.
2. Ашылған **Басқаша сақтау** терезесінде файлдың атауы мен сақтау жолын көрсетіңіз.
3. **Сақтау** түймесін басыңыз.

Жергілікті пайдаланушылардың құқықтары экспортталмайды.

Тапсырманы импорттау

Топтық тапсырмалар мен арнайы құрылғыларға арналған тапсырмаларды импорттай аласыз. Басқару серверінің тапсырмалары импорттау үшін қолжетімді емес.

Тапсырманы импорттау үшін:

1. Тапсырманы импорттау қажет тапсырмалар тізімін таңдаңыз:

   - Егер сіз тапсырманы топтық тапсырмалар тізіміне импорттағыңыз келсе, сізге қажет басқару тобының жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.

   - Егер сіз тапсырманы арнайы құрылғыларға арналған тапсырмалар тізіміне импорттағыңыз келсе, консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. Тапсырманы импорттаудың келесі тәсілдерінің бірін таңдаңыз:

   - Тапсырмалар тізімінің контекстік мәзірінде **Барлық тапсырмалар → Импорттау** тармағын таңдаңыз.

   - Тапсырмалар тізімін басқару блогындағы **Тапсырманы файлдан импорттау** сілтемесі арқылы.

3. Ашылған терезеде тапсырманы импорттағыңыз келетін файлдың жолын көрсетіңіз.

4. **Ашу** түймесін басыңыз.

   Нәтижесінде, импортталған тапсырма тапсырмалар тізімінде көрсетіледі.

Импортталған жаңа тапсырманың атауы бұрыннан бар тапсырманың атауымен бірдей болса, импортталған тапсырманың атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Тапсырмаларды түрлендіру

Kaspersky Security Center көмегімен Kaspersky бағдарламаларының алдыңғы нұсқаларының тапсырмаларын бағдарламалардың ағымдағы нұсқаларының тапсырмаларына түрлендіруге болады.

Түрлендіру келесі бағдарламалардың тапсырмалары үшін мүмкін:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

Тапсырмаларды түрлендіру үшін:

1. Консоль ағашында тапсырмаларды түрлендіргіңіз келетін Басқару серверін таңдаңыз.

2. Басқару серверінің контекстік мәзірінен **Барлық тапсырмалар → Саясаттар мен тапсырмаларды жаппай түрлендіру шебері** тармағын таңдаңыз.

   Нәтижесінде, саясаттар мен тапсырмаларды жаппай түрлендіру шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысының нәтижесінде бағдарламалардың алдыңғы нұсқаларының тапсырмаларының параметрлерін қолданатын жаңа тапсырмалар қалыптасады.

Тапсырманы қолмен іске қосу және тоқтату

Тапсырмаларды екі тәсілмен конфигурациялауға және тоқтатуға болады: тапсырманың контекстік мәзірінен және осы тапсырма тағайындалған клиент құрылғысының сипаттары терезесінде.

> KLAdmins тобына кіретін пайдаланушылар құрылғының контекстік мәзірінен топтық тапсырмаларды іске қосу.

Тапсырманы контекстік мәзірден немесе тапсырма сипаттары терезесінен іске қосу немесе тоқтату үшін:

1. Тапсырмалар тізімінен тапсырманы таңдаңыз.
2. Тапсырманы келесі тәсілдердің бірімен іске қосыңыз немесе тоқтатыңыз:
   - Тапсырманың контекстік мәзірінде **Іске қосу** немесе **Тоқтату** тармағын таңдаңыз.
   - Тапсырма сипаттары терезесінің **Жалпы** бөліміндегі **Іске қосу** немесе **Тоқтату** түймесін басу арқылы.

Тапсырманы контекстік мәзірден немесе клиент құрылғысы сипаттары терезесінен іске қосу немесе тоқтату үшін:

1. Құрылғылар тізімінен құрылғыны таңдаңыз.
2. Тапсырманы келесі тәсілдердің бірімен іске қосыңыз немесе тоқтатыңыз:
   - Құрылғының мәнмәтіндік мәзірінен **Барлық тапсырмалар** → **Тапсырманы іске қосу** тармағын таңдаңыз. Тапсырмалар тізімінен қажеттісін таңдаңыз.

     Тапсырма тағайындалған құрылғылардың тізімі таңдалған құрылғымен ауыстырылады. Тапсырма іске қосылды.
   - Құрылғы сипаттары терезесінің **Тапсырмалар** бөліміндегі бастау түймесін () немесе тоқтату түймесін () басу арқылы.

Тапсырманы қолмен тоқтата тұру және жалғастыру

Іске қосылған тапсырманы тоқтата тұру немесе жалғастыру үшін:

1. Тапсырмалар тізімінен тапсырманы таңдаңыз.
2. Тапсырманың орындалуын келесі тәсілдердің бірімен тоқтата тұрыңыз немесе жалғастырыңыз:
   - Тапсырманың контекстік мәзірінде **Кідірту** немесе **Жалғастыру** тармағын таңдаңыз.
   - Тапсырма сипаттары терезесінің **Жалпы** бөлімінде **Кідірту** немесе **Жалғастыру** түймесін басыңыз.

Тапсырманы орындау барысын бақылау

Тапсырманың орындалу барысын бақылау үшін,

тапсырма сипаттары терезесінде **Жалпы** бөлімін таңдаңыз.

Жалпы бөлімі терезесінің ортаңғы бөлігінде тапсырманың ағымдағы жағдайы туралы ақпарат бар.

Басқару серверінде сақталатын тапсырмаларды орындау нәтижелерін қарап шығу

Kaspersky Security Center сізге топтық тапсырмалардың нәтижелерін, арнайы құрылғыларға арналған тапсырмаларды және Басқару сервері тапсырмаларын көруге мүмкіндік береді.

Тапсырманы орындау нәтижелерін көру үшін келесі әрекеттерді орындаңыз:

1. Тапсырма сипаттары терезесінде **Жалпы** бөлімін таңдаңыз.
2. **Нәтижелер** сілтемесі арқылы **Тапсырма нәтижелері** терезесін ашыңыз.

Қосалқы Басқару серверіне арналған тапсырманың нәтижелерін көру үшін:

1. Тапсырма сипаттары терезесінде **Жалпы** бөлімін таңдаңыз.
2. **Нәтижелер** сілтемесі арқылы **Тапсырма нәтижелері** терезесін ашыңыз.
3. **Қосалқы серверлердің статистикасы** түймесін басыңыз.
4. **Тапсырма нәтижелері** терезесін көрсеткіңіз келетін қосалқы Серверді таңдаңыз.

Тапсырманы орындау нәтижелері туралы ақпарат сүзгісін конфигурациялау

Kaspersky Security Center сізге топтық тапсырмаларды, арнайы құрылғыларға арналған тапсырмаларды және Басқару сервері тапсырмаларын орындау нәтижелері туралы ақпаратты көруге мүмкіндік береді. Жергілікті тапсырмалар үшін сүзу қолжетімді емес.

Тапсырманы орындау нәтижелері туралы ақпарат алу мақсатымен сүзгіні орнату үшін:

1. Тапсырма сипаттары терезесінде **Жалпы** бөлімін таңдаңыз.
2. **Нәтижелер** сілтемесі арқылы **Тапсырма нәтижелері** терезесін ашыңыз.

   Терезенің жоғарғы жағындағы кестеде тапсырма тағайындалған барлық құрылғылардың тізімі бар. Терезенің төменгі жағындағы кестеде таңдалған құрылғыдағы тапсырманы орындау нәтижелері бар.

3. Сізді қызықтыратын кестеде тінтуірдің оң жақ түймесімен контекстік мәзірді ашып, ондағы **Сүзгі** тармағын таңдаңыз.

4. Ашылған **Сүзгіні қолдану** терезесінде сүзу параметрлерін **Оқиғалар**, **Құрылғылар** және **Уақыт** терезесінің бөлімдерінде конфигурациялаңыз. **OK** түймесін басыңыз.

Тапсырма нәтижелері терезесіндегі нәтижелер сүзгіде белгіленген параметрлерді қанағаттандыратын ақпарат көрсетіледі.

Тапсырманы өзгерту. Өзгерістерді шегіндіру

Тапсырманы өзгерту үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. **Тапсырмалар** қалтасының жұмыс аймағында тапсырманы таңдап, мәнмәтіндік мәзірдің көмегімен тапсырма сипаттары терезесіне өтіңіз.

3. Қажетті өзгерістер енгізіңіз.

   Тапсырма ауқымынан шығарып тастау бөлімінде тапсырма таралмайтын салынған топтар тізімін конфигурациялауға болады.

4. **Қолдану** түймесін басыңыз.

Тапсырма өзгерістері тапсырма сипаттары терезесінде, **Тексерістер журналы** бөлімінде сақталады.

Қажет болса, тапсырма өзгерістерін шегіндіре аласыз.

Тапсырма өзгерістерін шегіндіру үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. Өзгерістерін шегіндіру қажет болған тапсырманы таңдап, мәнмәтіндік мәзірдің көмегімен тапсырма сипаттары терезесіне өтіңіз.

3. Тапсырма сипаттары терезесінде **Тексерістер журналы** бөлімін таңдаңыз.

4. Тапсырманы тексеру тізімінде, өзгерістерін шегіндіру қажет болған тексеру нөмірін таңдаңыз.

5. **Кеңейтілген** түймесін басыңыз да, ашылатын тізімнен **Шегіндіру** мәнін таңдаңыз.

Тапсырмаларды салыстыру

Бір типтегі тапсырмаларды салыстыруға болады, мысалы, екі зиянды БҚ іздеу тапсырмасын салыстыруға болады, бірақ зиянды БҚ іздеу тапсырмасын жаңартуларды орнату тапсырмасымен салыстыруға болмайды. Тапсырмаларды салыстыру нәтижесінде сіз қандай тапсырма параметрлері сәйкес келетінін және қайсысы ерекшеленетінін көрсететін есеп аласыз. Тапсырмаларды салыстыру есебін басып шығаруға немесе файлға сақтауға болады. Бір компанияның әртүрлі бөлімшелері үшін бір типтегі әртүрлі тапсырмалар болған жағдайда, тапсырмаларды салыстыру қажет болуы мүмкін. Мысалы, бухгалтерия үшін зиянды бағдарламаны іздеу тапсырмасы құрылғылардың жергілікті дискілерінде ғана бар, ал қызметкерлері клиенттермен хат алмасатын сату тобы үшін жергілікті дискілерді де, поштаны да тексеру тапсырмасы бар. Мұндай айырмашылықтарды тез көру үшін тапсырманың барлық параметрлерін қараудың қажеті жоқ, тапсырмаларды салыстыру жеткілікті.

Салыстыруды тек бір типтегі тапсырмалар үшін орындауға болады.

Тапсырмаларды тек жұппен салыстыруға болады.

Сіз тапсырмаларды келесі тәсілдердің бірімен салыстыра аласыз: бір тапсырманы таңдап, оны екіншісімен салыстыру арқылы немесе тапсырмалар тізіміндегі кез келген екі тапсырманы салыстыру арқылы.

Бір тапсырманы таңдап, оны екіншісімен салыстыру үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Тапсырмалар** қалтасының жұмыс аймағында басқа тапсырмамен салыстыру қажет болған тапсырманы таңдаңыз.
3. Тапсырманың мәнмәтіндік мәзірінде **Барлық тапсырмалар → Басқа тапсырмамен салыстыру** тармағын таңдаңыз.
4. **Тапсырманы таңдау** терезесінде салыстырылатын тапсырманы таңдаңыз.
5. **OK** түймесін басыңыз.

HTML пішіміндегі екі тапсырманы салыстыру есебі көрсетіледі.

Тапсырмалар тізіміндегі екі тапсырманы салыстыру үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Тапсырмалар** қалтасында, тапсырмалар тізімінде **SHIFT** немесе **CTRL** пернесінің көмегімен бір типті екі тапсырманы таңдаңыз.
3. Мәнмәтіндік мәзірде **Салыстыру** тармағын таңдаңыз.

Таңдалған тапсырмаларды HTML пішімінде салыстыру есебі көрсетіледі.

Тапсырмаларды салыстыру кезінде, егер қолданылатын құпиясөздер әртүрлі болса, тапсырмаларды салыстыру есебінде ****** таңбалары көрсетіледі.

Тапсырманың сипаттарында құпиясөз өзгертілген болса, тапсырмаларды тексеруді салыстыру есебінде ****** таңбалары көрсетіледі.

Тапсырмаларды іске қосуға арналған есептік жазбалар

Сіз тапсырма іске қосылуы тиісті есептік жазбаны белгілей аласыз.

Мысалы, талап ету бойынша сканерлеу тапсырмаларын орындау үшін сканерленетін нысанға қатынасу құқықтары, ал жаңарту тапсырмаларын орындау үшін – авторизацияланған прокси-сервер пайдаланушысы құқықтары қажет. Тапсырманы іске қосу үшін есептік жазбаны белгілеу мүмкіндігі, егер тапсырманы іске қосқан пайдаланушының қажетті қатынасу құқықтары болмаса, талап ету бойынша сканерлеу тапсырмаларын және жаңарту тапсырмаларын орындау кезінде қателерді болдырмауға мүмкіндік береді.

Құрылғыда Желілік агент орнатылмаған немесе қолжетімсіз болса, бағдарламаны қашықтан орнату және жою тапсырмаларында, есептік жазба клиент құрылғыларына орнату (жою) үшін қажетті файлдарды жүктеу мақсатымен қолданылады. Желілік агент орнатылған және қолжетімді болған кезде, есептік жазба, тапсырманың параметрлеріне сәйкес файдарды жеткізу ортақ қатынасу қалтасындағы Microsoft Windows құралдарымен ғана орындалған жағдайда қолданылады. Бұл жағдайда, есептік жазба құрылғыда келесі құқықтарға ие болуы тиіс:

- бағдарламаларды қашықтан іске қосу құқығы;
- Admin$ ресурсына қатысты құқықтар;
- *Қызмет ретінде жүйеге кіру* құқығы.

Файлдарды құрылғыларға Желілік агент жеткізсе, есептік жазба қолданылмайды. Файлдарды көшіру және орнату бойынша барлық операцияларды **Желілік агент** (**LocalSystem есептік жазбасы**) орындайтын болады.

Тапсырманы орындау тарихын экспорттау

Тапсырмада қандай да бір мәселелерге тап болсаңыз, негізгі себептерді зерттеу қажет болуы мүмкін. Ол үшін тапсырманы орындау тарихын экспорттап, әрі қарай талдауға болады.

Тапсырманы орындау тарихын экспорттау үшін:

1. Құрылғыңыздағы каталогте бос TXT файлын жасаңыз.

   Тапсырманы орындау тарихы осы файлға экспортталады.

2. Тапсырма нәтижелері терезесін ашыңыз.

3. Тапсырма нәтижелері терезесінің жоғарғы бөлігінде мәселелері бар құрылғыны таңдаңыз.

4. Таңдалған құрылғының орындау тарихы көрсетілетін тапсырма нәтижелері терезесінің төменгі бөлігінде бір немесе бірнеше оқиғаны таңдаңыз.

   Бірнеше оқиғаны таңдау үшін **Shift** немесе **Ctrl** пернесін пайдаланыңыз.

5. Контекстік мәзірді ашу үшін таңдалған оқиғаларды тінтуірдің оң жақ түймесімен басып, **Экспорттау** опциясын таңдаңыз.

   Нәтижесінде, оқиғаларды экспорттау шебері іске қосылады.

6. Шебердің **Экспорттау файлы** қадамында **Шолу** түймесін басып, тапсырманы орындау тарихын экспорттау үшін жасалған TXT файлын таңдаңыз.

   Тек таңдалған оқиғаларды экспорттау керек болса, **Тек таңдалған оқиғаларды экспорттау** опциясын қосыңыз.

   Тапсырманы орындаудың бүкіл тарихын (барлық оқиғаны) экспорттағыңыз келсе, **Тек таңдалған оқиғаларды экспорттау** опциясы өшірілген болуы керек.

7. **Келесі** түймесін басыңыз.

8. Шебердің **Экспорттау пішімі** қадамында келесі опциялардың бірін қосыңыз:

   - **Табуляция таңбаларымен бөлінген Юникод пішіміндегі мәтін түрінде экспорттау**

     Экспортталған деректерде бірнеше тілдегі арнайы таңбалар мен белгілер болса және экспортталған деректері бар TXT файлы әртүрлі қолданбаларда ашылған кезде барлық таңбаның дәл сақталуын қамтамасыз ету қажет болса, осы опцияны қосыңыз.

   - **Табуляция таңбаларымен бөлінген мәтін түрінде экспорттау**

     Ескі жүйелермен немесе Юникодты қолдамайтын қолданбалармен үйлесімділікті сақтағыңыз келсе, осы опцияны қосыңыз.

9. Шебер жұмысын аяқтау үшін **Келесі** түймесін басыңыз.

Тапсырманы орындау тарихы таңдалған TXT файлына экспортталады.

Тапсырмалардың құпиясөзін өзгерту шебері

Жергілікті емес тапсырма үшін, сіз тапсырманы іске қосуға құқық беретін есептік жазбаны көрсете аласыз. Есептік жазбаны, тапсырманы жасау кезінде немесе қолданыстағы тапсырманың сипаттарында көрсетуге болады. Егер аталған есептік жазба ұйымда белгіленген қауіпсіздік ережелеріне сәйкес пайдаланылса, бұл ережелер есептік жазбаның құпиясөзін мезгіл-мезгіл өзгертуді талап етуі мүмкін. Есептік жазба құпиясөзінің мерзімі аяқталғаннан кейін және жаңа құпиясөзді орнатқаннан кейін, тапсырма сипаттарында жаңа жарамды құпиясөзді көрсеткенге дейін тапсырма іске қосылмайды.

Тапсырмалардың құпиясөзін өзгерту шебері, есептік жазба көрсетілген барлық тапсырмаларда ескі құпиясөзді жаңасына автоматты түрде тапсыруға мүмкіндік береді. Мұны әр тапсырманың сипаттарында қолмен жасауға болады.

Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу үшін:

1. Консоль ағашында **Тапсырмалар** түйінін таңдаңыз.

2. Басқару сервері түйінінің контекстік мәзірінде **Тапсырмалардың құпиясөзін өзгерту шебері** тармағын таңдаңыз.

Содан кейін, шебердің нұсқауларын орындаңыз.

1-қадам. Есептік деректерді таңдау

Есептік жазба және **Құпиясөз** өрістерінде сіздің жүйеңізде әрекет ететін жаңа есептік деректерді көрсетіңіз (мысалы, Active Directory жүйесінде). Шебердің келесі қадамына өткен кезде, Kaspersky Security Center бағдарламасы аталған есептік жазбаның атауы әрбір жергілікті емес тапсырманың сипаттарындағы есептік жазбаның атауына сәйкес келетіндігін тексереді. Егер есептік жазба атаулары сәйкес келсе, тапсырма сипаттарындағы құпиясөз автоматты түрде жаңасына ауысады.

Ескі құпиясөз (міндетті емес) өрісін толтырған кезде, Kaspersky Security Center бағдарламасы құпиясөзді тек атауы мен ескі құпиясөз мәндері сәйкес келетін тапсырмалар үшін ауыстырады. Ауыстыру автоматты түрде орындалады. Барлық басқа жағдайларда, шебердің келесі қадамында орындалатын әрекетті таңдау керек.

2-қадам. Орындалып жатқан әрекетті таңдау

Егер шебердің бірінші қадамында сіз ескі құпиясөзді көрсетпеген болсаңыз немесе көрсетілген ескі құпиясөз тапсырмалардың құпиясөздеріне сәйкес келмесе, онда сіз осы тапсырмалармен орындалатын әрекетті таңдауыңыз керек.

Мақұлдау қажет күйі бар әрбір тапсырма үшін, тапсырманың сипаттарында құпиясөзді жойғыңыз келетініңізді немесе оны жаңасына ауыстырғыңыз келетініңізді анықтаңыз. Егер сіз құпиясөзді жоюды таңдасаңыз, тапсырма әдепкі бойынша орнатылған есептік жазба құқықтарымен іске қосу режиміне өтеді.

3-қадам. Нәтижелерді қарап шығу

Шебердің соңғы қадамында анықталған тапсырмалардың әрқайсысының нәтижелерін қараңыз. Шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Виртуалды Басқару серверіне бағынатын басқару топтары иерархиясын жасау

Виртуалды Басқару сервері құрылғаннан кейін, ол әдепкі бойынша **Басқарылатын құрылғылар** басқару тобын қамтиды.

Виртуалды Басқару серверіне бағынатын басқару топтарының иерархиясын құру процедурасы физикалық Басқару серверіне бағынатын басқару топтарының иерархиясын құру процедурасына сәйкес келеді.

Виртуалды Басқару серверіне бағынатын басқару топтарының құрамына қосалқы және виртуалды Басқару серверлерін қосуға болмайды. Бұл виртуалды Басқару серверлері шектеулерімен байланысты.

Саясаттар және профильдер

Kaspersky Security Center Web Console бағдарламасында Kaspersky бағдарламаларына арналған саясаттарды жасауға болады. Бұл бөлімде саясаттар және профильдер сипатталған, сондай-ақ оларды жасау және өзгерту бойынша нұсқаулар келтірілген.

Саясаттар иерархиясы, саясат профильдерін қолдану

Осы бөлім саясаттарды басқару топтарындағы құрылғыларға қолдану ерекшеліктері туралы ақпаратты қамтиды. Осы бөлім саясаттардың профильдері туралы ақпаратты да қамтиды.

Саясаттар иерархиясы

Kaspersky Security Center-де саясаттар көптеген құрылғыларда бірдей параметрлер жинағын белгілеуге арналған. Мысалы, G тобы үшін анықталған P бағдарламасы саясатының әрекет ету ауқымы сипаттарында **Тектік топтан иелену** жалаушасы алынған ішкі топтарды қоспағанда, G басқару тобында және барлық оның ішкі топтарында орналасқан P бағдарламасы орнатылған басқарылатын құрылғылар болып табылады.

Саясат оның ішіндегі параметрлердің жанында "құлыптардың" (🔒) болуымен жергілікті параметрлерден ерекшеленеді. Саясат сипаттарында орнатылған құлып оған сәйкес параметр (немесе параметрлер тобы) біріншіден, тиімді параметрлерді қалыптастырған кезде пайдаланылуы керектігін, екіншіден, төмендегі саясатқа жазылуы керектігін білдіреді.

Құрылғыда әрекет ететін параметрлерді қалыптастыруды келесі түрде көрсетуге болады: саясаттан құлпы орнатылмаған параметрлердің мәндері алынады, кейін олардың үстіне жергілікті параметрлердің мәндері жазылады, кейін алған мәндердің үстіне саясаттан алынған құлпы орнатылған параметрлердің мәндері жазылады.

Бірдей бағдарламаның саясаттары бір-біріне басқару топтарының иерархиясы бойынша әрекет етеді: жоғарыдағы саясаттың орнатылған құлпы бар параметрлері төмендегі саясаттың аттас параметрлерін қайта жазады.

Ерекше саясат түрі бар - автономды пайдаланушыларға арналған саясат. Бұл саясат құрылғы автономды режимге ауысқан кезде құрылғыда күшіне енеді. Автономды пайдаланушыларға арналған саясаттар басқа саясаттарға басқару топтарының иерархиясы бойынша әрекет етпейді.

Саясат профильдері

Тек қана басқару топтарының иерархиясына сүйене отырып құрылғыларға саясаттарды қолдану көптеген жағдайларда ыңғайсыз. Әртүрлі басқару топтары үшін саясаттың бірнеше көшірмелерін жасау және одан әрі осы саясаттардың мазмұнын қолмен синхрондау қажеттілігі туындауы мүмкін.

Осындай мәселелерді болдырмауға көмектесу үшін, Kaspersky Security Center *саясаттар профильдерін* қолдайды. Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер клиент құрылғысында (компьютерде, ұялы құрылғыда) әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды. Профильді белсендірген кезде, профиль белсендірілгенге дейін құрылғыда әрекет еткен саясат параметрлері өзгереді. Бұл параметрлер профильде көрсетілген мәндерді қабылдайды.

Саясаттардың профильдері қазір келесі шектеулерге ие:

- саясатта ең көбі 100 профиль болуы мүмкін;
- саясаттың профилі басқа профильдерді қамти алмайды;
- саясаттың профилі хабарландыру параметрлерін қамти алмайды.

Профильдің мазмұны

Саясаттың профилі келесі құрамдас бөліктерді қамтиды:

- Атауы. Атаулары бірдей профильдер бір-біріне ортақ ережелері бар басқару топтарының иерархиясы арқылы әсер етеді.
- Саясат параметрлерінің қосалқы жиынтығы. Барлық параметрлері бар саясатқа қарағанда, профильде шынымен керек (құлып орнатылған) параметрлер ғана бар.
- Белсендіру шарты – құрылғы сипаттарының логикалық өрнегі. Профиль профильді белсендіру шарты шынайы болған кезде ғана белсенді (саясатты толықтырады). Қалған жағдайларда профиль белсенді емес және ескерілмейді. Логикалық өрнекте құрылғының келесі сипаттары қатыса алады:
  - автономды режим күйі;
  - желілік орта сипаттары – Желілік агентті қосудың белсенді ережесінің атауы;
  - құрылғыда көрсетілген тегтердің болуы немесе болмауы;
  - Active Directory бөлімшесінде құрылғының орналасқан жері: айқын (құрылғы тікелей көрсетілген бөлімшеде орналасқан) немесе айқын емес (құрылғы кез келген тіркеме деңгейінде көрсетілген бөлімшенің ішінде орналасқан бөлімшеде орналасқан);
  - құрылғының Active Directory қауіпсіздік тобындағы мүшелігі (айқын немесе айқын емес);
  - құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі (айқын немесе айқын емес).
- Профильді сөндіру жалаушасы. Сөндірілген профильдер әрқашан ескерілмейді, оларды белсендіру шарттары шынайылыққа тексерілмейді.
- Профильдің басымдығы. Профильдерді белсендіру шарттары тәуелсіз, сондықтан бір уақытта бірден бірнеше профильдер белсендірілуі мүмкін. Егер белсенді профильдер параметрлердің талассыз жинақтарын қамтыса, онда ешқандай мәселелер туындамайды. Дегенмен екі белсенді профильде бірдей параметрдің әртүрлі мәндері болса, түсініксіздік орын алады. Бұл түсініксіздікке профиль басымдықтары арқылы жол бермеу керек: түсініксіздік айнымалысының мәні басымдығы жоғарырақ профильден (профильдер тізімінде жоғары бағаланған) алынады.

Саясаттар иерархия бойынша бір-біріне әрекет еткен кезде профильдердің жағдайы

Аттас профильдер саясаттарды біріктіру ережелеріне сәйкес біріктіріледі. Жоғарғы саясаттың профильдері төменгі саясаттың профильдерінен басымдырақ. Егер "жоғарғы" саясатта параметрлерді өзгертуге тыйым салынса (құлып батырмасы басылған), "төменгі" саясатта "жоғарғы" саясаттағы профильді белсендіру шарттары пайдаланылады. Егер "жоғарғы" саясатта параметрлерді өзгертуге рұқсат етілсе, онда "төменгі" саясаттағы профильді белсендіру шарттары пайдаланылады.

Саясат профилі белсендіру шартында **Құрылғы офлайн режимде** қамти алғандықтан, профиль одан әрі қолдау көрсетілмейтін автономды пайдаланушылар үшін саясаттардың функционалдығын толығымен ауыстырады.

Автономды пайдаланушыларға арналған саясат профильдерді қамтуы мүмкін, бірақ оның профильдерін белсендіру құрылғы автономды режимге ауыспайынша туындамайды.

Саясат параметрлерін иелену

Саясат басқару топтарына белгіленеді. Саясат параметрлерін *иеленуге* болады, яғни ол құрылған басқару топтарының ішкі топтарына (еншілес топтарына) берілуі мүмкін. Тектік топ үшін жасалған саясат *тектік саясат* деп те аталады.

Параметрлерді негізгі саясаттан иелену және **Параметрлерді еншілес саясаттардың иеленуін жылдамдату** параметрлерін қосуға немесе өшіруге болады.

- Еншілес саясат үшін **Параметрлерді негізгі саясаттан иелену** параметрін қосып, негізгі саясатта кейбір параметрлерді бұғаттаған болсаңыз, осы параметрлерді еншілес топ үшін өзгерте алмайсыз. Алайда, сіз ата-ана саясатында бұғаталмаған параметрлерді өзгерте аласыз.

- Еншілес саясат үшін **Параметрлерді негізгі саясаттан иелену** параметрін өшірген болсаңыз, онда сіз негізгі саясатта кейбір параметрлер бұғатталған болса да, еншілес топтағы барлық параметрлерді өзгерте аласыз.

- Тектік топта **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену** параметрі қосулы болса, бұл әрбір еншілес саясат үшін **Параметрлерді негізгі саясаттан иелену** параметрін қосады. Бұл жағдайда, сіз осы параметрді еншілес саясат үшін өшіре алмайсыз. Негізгі саясатта бұғатталған барлық параметрлер еншілес топтарда мәжбүрлеп иеленеді және сіз бұл параметрлерді еншілес топтарда өзгерте алмайсыз.

- **Басқарылатын құрылғылар** тобы үшін саясаттарда **Параметрлерді негізгі саясаттан иелену** параметрі ешқандай параметрлерге әсер етпейді, себебі **Басқарылатын құрылғылар** тобында жоғары тұрған топтар жоқ және демек, ол ешқандай саясатты иеленбейді.

Әдепкі бойынша **Параметрлерді негізгі саясаттан иелену** параметрі жаңа саясат үшін қосулы.

Егер саясатта профильдер болса, барлық еншілес саясаттар осы профильдерді иеленеді.

Саясатты басқару

Клиент құрылғыларында орнатылған бағдарламалардың параметрлерін орталықтандырылған конфигурациялау саясатты анықтау арқылы жүзеге асырылады.

Басқару тобындағы бағдарламалар үшін құрылған саясаттар жұмыс аймағында **Саясаттар** қойыншасында көрсетіледі. Әр саясат атауының алдында оның күйін сипаттайтын белгіше көрсетіледі.

Саясат жойылғаннан немесе тоқтатылғаннан кейін бағдарлама саясатта белгіленген параметрлермен жұмысын жалғастырады. Болашақта бұл параметрлерді қолмен өзгертуге болады.

Саясатты қолдану келесідей жүзеге асырылады: егер құрылғыда резиденттік тапсырмалар (тұрақты қорғау тапсырмалары) орындалса, олардың орындалуы параметрлердің жаңа мәндерімен жалғасады. Іске қосылған мерзімді тапсырмалар (талап ету бойынша тексеру, бағдарлама дерекқорларын жаңарту) өзгермеген мәндермен орындалады. Мерзімді тапсырмаларды жаңа іске қосу параметрлердің өзгертілген мәндерімен жүзеге асырылады.

Көптиістілікті қолдайтын бағдарламаларға арналған саясаттар төменгі деңгейдегі басқару топтары, сондай-ақ жоғарғы деңгейдегі басқару топтары үшін иеленеді: саясат бағдарлама орнатылған барлық клиент құрылғыларына қатысты қолданылады.

Басқару серверлерінің иерархиялық құрылымын пайдаланған жағдайда, қосалқы Серверлер негізгі Басқару серверінен саясаттарды алады және оларды клиент құрылғыларына таратады. Иелену механизмі қосылған кезде саясат параметрлерін негізгі Басқару серверінде өзгертуге болады. Осыдан кейін, саясат параметрлеріне енгізілген өзгерістер қосалқы Басқару серверлеріндегі иеленген саясатқа қолданылады.

Негізгі және қосалқы Басқару серверлері арасындағы байланыс үзілген кезде, қосалқы Сервердегі саясат бұрынғы параметрлермен жұмыс істеуді жалғастырады. Негізгі Басқару серверінде өзгертілген саясат параметрлері қосылымды қалпына келтіргеннен кейін қосалқы Серверге таралады.

Иелену механизмі өшірілген кезде саясат параметрлерін басты Серверге қарамастан қосалқы Серверде өзгертуге болады.

Басқару сервері мен клиент құрылғысы арасында байланыс үзілсе, құрылғыда автономды пайдаланушыға арналған саясат күшіне енеді (егер ол анықталған болса) немесе байланыс қалпына келтірілгенге дейін саясат бұрынғы параметрлермен жалғасады.

Саясатты қосалқы Басқару серверлеріне тарату нәтижелері негізгі Басқару серверіндегі саясат сипаттары терезесінде көрсетіледі.

Клиент құрылғыларына саясатты тарату нәтижелері, олар қосылған Басқару сервері саясатының сипаттар терезесінде көрсетіледі.

> Саясаттар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Саясатты жасау

Басқару консолінде саясатты тікелей саясат жасалатын басқару тобының қалтасында және **Саясаттар** қалтасының жұмыс аймағында жасауға болады.

Басқару топтары қалтасында саясат құру үшін:

1. Консоль ағашында саясат жасау үшін басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. **Жаңа саясат** түймесі бойынша саясат жасау шеберін іске қосыңыз.

Нәтижесінде, саясат жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Саясаттар қалтасының жұмыс аймағында саясат жасау үшін:

1. Консоль ағашында **Саясаттар** қалтасын таңдаңыз.
2. **Жаңа саясат** түймесі бойынша саясат жасау шеберін іске қосыңыз.

   Нәтижесінде, саясат жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Топтағы бір бағдарлама үшін бірнеше саясатты жасауға болады, бірақ олардың біреуі ғана белсенді бола алады. Жаңа белсенді саясатты құру кезінде алдыңғы белсенді саясат белсенді емес болады.

Саясатты құру кезінде, бағдарламаны іске қосатын параметрлердің ең аз жиынтығын конфигурациялауға болады. Параметрлердің қалған мәндері әдепкі бойынша орнатылады және бағдарламаны жергілікті орнатқан кезде әдепкі бойынша мәндерге сәйкес келеді. Саясатты жасағаннан кейін, оны өзгертуге болады.

Саясаттар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Саясатты қолданғаннан кейін өзгеретін Kaspersky бағдарламаларының параметрлері олардың әрқайсысының нұсқауларында егжей-тегжейлі сипатталған.

Саясатты жасағаннан кейін өзгертуге тыйым салынған параметрлер ("құлып" орнатылған), бағдарлама үшін қандай параметрлер бұрын анықталғанына қарамастан, клиент құрылғыларында әрекет ете бастайды.

Салынған топта иеленген саясатты көрсету

Салынған басқару тобына арналған иеленген саясаттарды көрсетуді қосу үшін:

1. Консоль ағашында иеленген саясаттарды көрсету үшін басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. Саясаттар тізімінің контекстік мәзірінде **Көру** → **Иеленген саясаттар** тармағын таңдаңыз.

   Нәтижесінде, иеленген саясаттар келесі белгішесі бар саясат тізімінде көрсетіледі:

- – егер олар негізгі Басқару серверінде құрылған топтан иеленген болса;
- – егер олар жоғарғы деңгейдегі топтан иеленген болса.

  Параметрлерді иелену режимі қосылған кезде, иеленген саясатты өзгерту олар құрылған топта ғана қолжетімді. Мұрагерлік саясатты өзгерту саясатты иеленетін топта қолжетімді емес.

Саясатты белсендіру

Таңдалған топқа арналған саясатты белсенді ету үшін:

1. **Саясаттар** қойыншасындағы топтың жұмыс аймағында белсенді ету қажет саясатты таңдаңыз.
2. Саясатты белсендіру үшін келесі әрекеттердің бірін орындаңыз:
   - Саясаттың мәнмәтіндік мәзірінде **Белсенді саясат** тармағын таңдаңыз.
   - Саясат сипаттары терезесінде **Жалпы** бөлімін ашып, **Саясаттың күйі** параметрлер тобынан **Белсенді саясат** опциясын таңдаңыз.

Нәтижесінде, саясат таңдалған басқару тобы үшін белсенді болады.

Клиент құрылғыларының көп санына саясатты қолданған кезде Басқару серверіне түсетін жүктеме және желілік трафик көлемі біраз уақытқа айтарлықтай артады.

"Вирустық шабуыл" оқиғасы бойынша саясатты автоматты түрде белсендіру

"Вирустық шабуыл" оқиғасы басталған кезде саясат автоматты түрде белсендірілді:

1. Басқару сервері сипаттары терезесінде **Вирустық шабуыл** бөлімін ашыңыз.
2. **Вирустық шабуыл оқиғасы орын алған кезде белсендірілетін саясаттарды конфигурациялау** сілтемесі арқылы **Саясаттарды белсендіру** терезесін ашып, вирустық шабуыл кезінде белсендірілетін таңдалған саясаттар тізіміне саясатты қосыңыз.

Вирустық шабуыл оқиғасы бойынша саясат белсендірілген жағдайда, алдыңғы саясатқа тек қолмен оралуға болады.

Автономды пайдаланушылар саясатын қолдану

Автономды пайдаланушыларға арналған саясат, ұйым желісінен ажыратылған жағдайда құрылғыда күшіне енеді.

Автономды пайдаланушыларға саясатты қолдану үшін:

саясат сипаттары терезесінде **Жалпы** бөлімін ашып, **Саясаттың күйі** параметрлер блогында **Автономды пайдаланушылар саясаты** нұсқасын таңдаңыз.

Нәтижесінде, автономды пайдаланушыларға арналған саясат ұйым желісінен ажыратылған жағдайда құрылғыларда әрекет ете бастайды.

Саясатты өзгерту. Өзгерістерді шегіндіру

Саясатты өзгерту үшін:

1. Консоль ағашында **Саясаттар** қалтасын таңдаңыз.
2. **Саясаттар** қалтасының жұмыс аймағында саясатты таңдап, мәнмәтіндік мәзірдің көмегімен саясат сипаттары терезесіне өтіңіз.
3. Қажетті өзгерістер енгізіңіз.
4. **Қолдану** түймесін басыңыз.

Саясат өзгерістері саясаттың сипаттарында, **Тексерістер журналы** бөлімінде сақталады.

Қажет болса, саясат өзгерістерін шегіндіре аласыз.

Саясат өзгерістерін шегіндіру үшін:

1. Консоль ағашында **Саясаттар** қалтасын таңдаңыз.
2. Өзгерістерін шегіндіру қажет болған саясатты таңдап, мәнмәтіндік мәзірдің көмегімен саясат сипаттары терезесіне өтіңіз.
3. Саясат сипаттары терезесінде **Тексерістер журналы** бөлімін таңдаңыз.
4. Саясатты тексеру тізімінде, өзгерістерін шегіндіру қажет болған тексеру нөмірін таңдаңыз.
5. **Кеңейтілген** түймесін басыңыз да, ашылатын тізімнен **Шегіндіру** мәнін таңдаңыз.

Саясаттарды салыстыру

Бір басқарылатын бағдарлама үшін екі саясатты салыстыруға болады. Саясатты салыстыру нәтижесінде сіз қандай саясат параметрлері сәйкес келетінін және қайсысы ерекшеленетінін көрсететін есеп аласыз. Саясатты салыстыру, мысалы, жергілікті кеңселердегі әртүрлі әкімшілер бір басқарылатын бағдарлама үшін бірнеше саясат жасаған болса немесе әр жергілікті кеңсе үшін бір жоғарғы деңгейлі саясат иеленген болса және өзгертілсе қажет болуы мүмкін. Сіз саясаттарды келесі тәсілдердің бірімен салыстыра аласыз: бір саясатты таңдап, оны екіншісімен салыстыру арқылы немесе саясаттар тізіміндегі кез келген екі саясатты салыстыру арқылы.

Тексеру тарихында ағымдағы түзетулері бар саясаттарды ғана салыстыруға болады.

Бір саясатты екіншісімен салыстыру үшін:

1. Консоль ағашында **Саясаттар** қалтасын таңдаңыз.
2. **Саясаттар** қалтасының жұмыс аймағында басқа саясатпен салыстыру қажет болған саясатты таңдаңыз.
3. Саясаттың мәнмәтіндік мәзірінде **Саясатты басқа саясатпен салыстыру** тармағын таңдаңыз.

4. **Саясатты таңдау** терезесінде салыстыру қажет болған саясатты таңдаңыз.

5. **OK** түймесін басыңыз.

Бағдарлама үшін HTML пішімінде екі саясатты салыстыру есебі көрсетіледі.

Саясат тізіміндегі екі саясатты салыстыру үшін:

1. Саясат тізіміндегі **Саясаттар** қалтасында **SHIFT** немесе **CTRL** пернесінің көмегімен бір басқарылатын бағдарлама үшін екі саясатты таңдаңыз.

2. Мәнмәтіндік мәзірде **Салыстыру** тармағын таңдаңыз.

Бағдарлама үшін HTML пішімінде екі саясатты салыстыру есебі көрсетіледі.

Kaspersky Endpoint Security for Windows бағдарламасының саясат параметрлерін салыстыру есебінде саясат профильдерін салыстыру да орындалады. Саясат профильдерінің параметрлерін салыстыру нәтижелерін азайтуға болады. Блокты азайту үшін блоктың атауы жанындағы көрсеткі белгішесін (▲) басыңыз.

Саясатты қолдану күйінің диаграммасын қарау

Kaspersky Security Center бағдарламасында әрбір құрылғыда саясатты қолдану нәтижелерін көруге болады.

Әр құрылғыда саясатты қолдану күйін көру үшін:

1. Топтың жұмыс аймағындағы **Саясаттар** қойындысында тарату күйін көргіңіз келетін саясатты таңдаңыз.

   Оң жақ тақтадағы диаграмма саясатты қолдану күйін көрсетеді.

2. **Мәліметтер** түймесін басыңыз.

   Саясатты қолдану нәтижелері терезесі ашылады.

   Саясатты қолдану нәтижелерін CSV немесе TXT файл пішіміне экспорттай аласыз.

Саясатты жою

Саясатты жою үшін:

1. Басқару тобының жұмыс аймағында **Саясаттар** қойыншасынан жойылатын саясатты таңдаңыз.

2. Саясатты келесі тәсілдердің бірімен жойыңыз:

   - Саясаттың мәнмәтіндік мәзірінде **Жою** тармағын таңдаңыз.

   - Таңдалған саясаттың ақпараттық терезесінде **Саясатты жою** сілтемесінен өтіңіз.

Саясатты көшіру

Саясатты көшіру үшін:

1. Өзіңізге қажетті топтың жұмыс аймағындағы **Саясаттар** қойыншасында саясатты таңдаңыз.
2. Саясаттың мәнмәтіндік мәзірінде **Көшіру** тармағын таңдаңыз.
3. Консоль ағашынан саясат қосуды қажет ететін топты таңдаңыз.

   Саясатты өзі көшірілген топқа қосуға болады.
4. Таңдалған топқа арналған саясат тізімінің контекстік мәзірінде **Саясаттар** қойыншасында **Кірістіру** тармағын таңдаңыз.

Нәтижесінде, саясат барлық параметрлерді сақтай отырып көшіріледі және ол тасымалданатын топтың құрылғыларына қолданылады. Егер сіз саясатты өзі көшірілген топқа салып жатсаңыз, индекс **(<келесі реттік сан>)** саясаттың атауына қосылады, мысалы: **(1)**, **(2)**.

Көшіру кезінде белсенді саясат белсенді болмайды. Қажет болса, оны белсенді ете аласыз.

Саясатты экспорттау

Саясатты экспорттау үшін:

1. Саясатты келесі тәсілдердің бірімен экспорттаңыз:
   - Саясаттың контекстік мәзірінде **Барлық тапсырмалар** → **Экспорттау** тармағын таңдаңыз.
   - Таңдалған саясаттың ақпараттық терезесінде **Саясатты файлға экспорттау** сілтемесінен өтіңіз.
2. Ашылған **Басқаша сақтау** терезесінде саясат файлының атауы мен жолын көрсетіңіз. **Сақтау** түймесін басыңыз.

Саясатты импорттау

Саясатты импорттау үшін:

1. Сізге қажет топтың жұмыс аймағында **Саясаттар** қойыншасында саясатты импорттаудың келесі тәсілдерінің бірін таңдаңыз:
   - Саясаттар тізімінің контекстік мәзірінде **Барлық тапсырмалар** → **Импорттау** тармағын таңдаңыз.
   - Саясаттар тізімін басқару блогындағы **Саясатты файлдан импорттау** түймесі арқылы.
2. Ашылған терезеде саясатты импорттағыңыз келетін файлдың жолын көрсетіңіз. **Ашу** түймесін басыңыз.

Импортталған саясат саясаттар тізімінде көрсетіледі. Сондай-ақ, саясат параметрлері мен профильдері импортталады. Экспортта таңдалған саясаттың күйіне қарамастан, импортталатын саясат белсенді емес. Саясат сипаттарындағы саясаттың күйін өзгертуге болады.

Импортталған жаңа саясаттың атауы бұрыннан бар саясаттың атауымен бірдей болса, импортталған саясаттың атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Саясаттарды түрлендіру

Kaspersky Security Center бағдарламасы Kaspersky басқарылатын бағдарламаларының алдыңғы нұсқаларының саясатын осы бағдарламалардың ағымдағы нұсқаларының саясатына айналдыра алады. Түрлендірілген саясаттар жаңартуға дейін орнатылған ағымдағы әкімші параметрлерін сақтайды, сонымен қатар бағдарламалардың ағымдағы нұсқаларынан жаңа параметрлерді қамтиды. Саясат басқарылатын Kaspersky қолданбасының жаңартылған нұсқасына түрлендірілсе, қолданба плагинінің алдыңғы нұсқасы орнатылған басқару серверіндегі саясатты ашу мүмкін емес. Kaspersky бағдарламаларын басқару плагиндері осы бағдарламалардың саясатын түрлендіруге болатындығын анықтайды. Әрбір қолдау көрсетілетін Kaspersky бағдарламасы үшін саясатты түрлендіру туралы ақпаратты келесі тізімнен тиісті анықтамадан қараңыз:

- **Жұмыс станцияларына арналған Kaspersky бағдарламалары:**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (орталықтан орналастыруға қолдау көрсетілмейді)
- **Ұялы құрылғылар үшін Kaspersky қолданбалары**:
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **Файл серверлеріне арналған Kaspersky бағдарламалары**:
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux

- **Виртуалды машиналарға арналған Kaspersky бағдарламалары:**
  - Kaspersky Security for Virtualization Жеңіл агент
  - Kaspersky Security for Virtualization Агентсіз қорғаныс
- **Мақсатты шабуылдарды анықтауға арналған Kaspersky бағдарламалары**:
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **KasperskyOS операциялық жүйесі орнатылған құрылғыларға арналған Kaspersky бағдарламалары**:
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (Kaspersky Thin Client үшін плагин)

Саясаттарды түрлендіру үшін:

1. Консоль ағашында саясатты түрлендіргіңіз келетін Басқару серверін таңдаңыз.
2. Басқару серверінің контекстік мәзірінен **Барлық тапсырмалар → Саясаттар мен тапсырмаларды жаппай түрлендіру шебері** тармағын таңдаңыз.

   Нәтижесінде, саясаттар мен тапсырмаларды жаппай түрлендіру шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысы аяқталғаннан кейін, әкімші саясатының ағымдағы параметрлерін және Kaspersky бағдарламаларының өзекті нұсқаларынан жаңа параметрлерді қолданатын саясаттар жасалады.

Саясат профильдерін басқару

Саясат профилі – бұл құрылғы берілген белсендіру ережелерін қанағаттандырса, клиент құрылғысында (компьютерде, ұялы құрылғыда) іске қосылатын аталған саясат параметрлерінің жиынтығы. Профильді белсендірген кезде, профиль белсендірілгенге дейін құрылғыда әрекет еткен саясат параметрлері өзгереді. Бұл параметрлер профильде көрсетілген мәндерді қабылдайды.

Саясат профильдері, бір басқару тобындағы құрылғылардың әртүрлі саясат параметрлері болуы үшін қажет. Мысалы, кейбір құрылғыларға арналған басқару тобында саясат параметрлерін өзгерту қажет болатын жағдай туындауы мүмкін. Бұл жағдайда, мұндай саясат үшін саясат профильдерін конфигурациялауға болады, оларды пайдалану арқасында басқару тобының барлық құрылғылары үшін саясат параметрлерін өзгертуге мүмкіндік беріледі. Мысалы, саясат "Пайдаланушылар" басқару тобының барлық құрылғылары үшін қалалық навигация бағдарламаларын іске қосуға тыйым салады. GPS навигациясының бағдарламалық жасақтамасы пайдаланушылардың басқару тобындағы курьер ретінде жұмыс істейтін пайдаланушы иелік ететін бір құрылғыда ғана қажет. Бұл құрылғыда "Курьер" тегін орнатуға және саясаттың барлық басқа параметрлерін сақтай отырып, тек "Курьер" тегі бар құрылғыда қалалық навигация бағдарламаларын іске қосуға рұқсат етілетіндей етіп саясат профилін конфигурациялауға болады. Бұл жағдайда, "Пайдаланушылар" басқару тобында "Курьер" тегі бар құрылғы пайда болса, онда қалалық навигация бағдарламаларын іске қосуға рұқсат етіледі. "Курьер" тегі жоқ "Пайдаланушылар" әкімшілік тобындағы басқа құрылғыларда қалалық навигация бағдарламаларын іске қосуға тыйым салынады.

Профильдерге тек келесі саясаттар үшін қолдау көрсетіледі:

- Kaspersky Endpoint Security for Windows саясаттары;
- Kaspersky Endpoint Security for Mac саясаттары;
- 10 Service Pack 1 нұсқасынан 10 Service Pack 3 Maintenance Release 1 нұсқасына дейінгі Kaspersky Mobile Device Management плагині саясаттары;
- Kaspersky Device Management for iOS плагині саясаттары;
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows саясаттары;
- Kaspersky Security for Virtualization 5.1 Light Agent for Linux саясаттары.

Саясат профильдері саясат қолданылатын клиент құрылғыларын басқаруды жеңілдетеді:

- Саясат профилінің параметрлері саясаттың өзінен өзгеше болуы мүмкін.
- Бір саясаттың бірнеше көшірмелерін қолдаудың және қолмен қолданудың қажеті жоқ, олар аз ғана параметрлермен ерекшеленеді.
- Автономды пайдаланушылар үшін бөлек саясат қажет емес.
- Сіз саясат профильдерін экспорттай және импорттай аласыз, сондай-ақ бұрыннан бар профильдер негізінде жаңа профильдер жасай аласыз.
- Бір саясат үшін бірнеше саясат профильдері белсенді болуы мүмкін. Құрылғыға осы құрылғыдағы белсендіру ережелерін қанағаттандыратын профильдер қолданылады.
- Профильдер саясат иерархиясына бағынады. Иеленген саясатта жоғарғы деңгейдегі барлық саясат профильдері бар.

Профильдер басымдықтары

Саясат үшін жасалған профильдер басымдықтың кему тәртібімен реттелген. Мысалы, егер X профилі профильдер тізіміндегі Y профилінен жоғары болса, онда X профилі Y профиліне қарағанда жоғары басымдыққа ие. Бір құрылғыға бір уақытта бірнеше профиль қолданылуы мүмкін. Егер қандай да бір параметрдің мәні профильдерде әртүрлі болса, құрылғыда жоғары басымдыққа ие профильдегі параметр мәні қолданылады.

Профильді белсендіру ережесі

Саясат профилі белсендіру ережесін орындау кезінде клиент құрылғысында белсендіріледі. *Белсендіру ережелері* – саясат профилі құрылғыда жұмыс істей бастайтын шарттар жиынтығы. Белсендіру ережесі келесі шарттарды қамтуы мүмкін:

- Клиент құрылғысындағы Желілік агент Серверге белгілі бір қосылым параметрлерінің жиынтығымен қосылады, мысалы, Сервер мекенжайы, порт нөмірі және т.б.
- Клиент құрылғысы автономды режимде.
- Клиент құрылғысына белгілі бір тегтер тағайындалады.
- Клиент құрылғысы анық (құрылғы тікелей көрсетілген бөлімшеде орналасқан) немесе анық емес түрде (құрылғы кез келген тіркеме деңгейіндегі көрсетілген бөлімшеде орналасқан) белгілі бір Active Directory бөлімшесінде орналасқан, құрылғы немесе оның иесі Active Directory қауіпсіздік тобында орналасқан.
- Клиент құрылғысы белгілі бір иесіне тиесілі немесе құрылғының иесі Kaspersky Security Center ішкі қауіпсіздік тобында орналасқан.
- Клиент құрылғының иесіне белгілі бір рөл тағайындалды.

Басқару топтары иерархиясындағы саясаттар

Егер сіз төменгі деңгейдегі басқару тобында саясат жасасаңыз, онда жаңа саясат жоғарғы деңгейдегі топ үшін белсенді саясат профильдерін иеленеді. Бірдей аттары бар профильдер біріктіріледі. Аса жоғары деңгейлі топқа арналған саясат профильдері аса жоғары басымдыққа ие. Мысалы, *A* басқару тобында *P(A)* саясаты басымдықтың кемуі тәртібінде *X1*, *X2* және *X3* профильдеріне ие. *A* тобының ішкі тобы болып табылатын *B* басқару тобында *X2*, *X4*, *X5* профильдеріне ие *P(B)* саясаты жасалған. Онда, *P(B)* саясатын *P(A)* саясаты өзгертеді, осылайша *P(B)* саясатындағы профильдер тізімі кему тәртібінде *X1*, *X2*, *X3*, *X4*, *X5* болады. *X2* саясатының профилі *P(B)* саясатының *X2* бастапқы күйіне және *P(A)* саясатының *X2* бастапқы күйіне байланысты болады. *P(B)* саясаты жасалғаннан кейін, *P(A)* саясаты *B* ішкі тобында көрсетілмейді.

Белсенді саясат, Желілік агент іске қосылған сайын, автономды режимді қосқан және өшірген кезде және клиент құрылғысына тағайындалған тегтер тізімін өзгерткен сайын қайта есептеледі. Мысалы, құрылғының жедел жад көлемі ұлғайтылды, нәтижесінде жедел жад көлемі үлкен құрылғылар үшін қолданылатын саясат профилі белсендірілді.

Саясат профилінің сипаттары мен шектеулері

Профильдер келесі сипаттарға ие:

- Белсенді емес саясат профильдері клиент құрылғыларына әсер етпейді.
- Егер саясат үшін **Автономды пайдаланушылар саясаты** күйі орнатылса, құрылғы корпоративтік желіден ажыратылған кезде саясат профильдері де қолданылады.
- Профильдер орындалатын файлдарға қатынасуды статикалық талдауды қолдамайды.

- Саясат профилінде оқиғалар туралы ескертулер параметрлері болмауы мүмкін.
- Егер құрылғыны Басқару серверіне қосу үшін 15000 UDP порты пайдаланылса, онда құрылғыға тег тағайындалған кезде тиісті саясат профилі бір минут ішінде белсендіріледі.
- Саясат профилін белсендіру ережелерін жасап жатқан кезде, Желілік агентті Басқару серверіне қосу ережелерін қолдана аласыз.

Саясат профилін жасау

Профиль жасау тек келесі бағдарламалардың саясаттары үшін қолжетімді:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows және одан жоғары;
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac;
- 10 Service Pack 3 Maintenance Release 1 нұсқаларына дейінгі Kaspersky Mobile Device Management плагині;
- Kaspersky Device Management for iOS плагині;
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows / Linux.

Саясат профилін жасау үшін:

1. Консоль ағашында саясат профилін жасау үшін саясаты бар басқару тобын таңдаңыз.
2. Басқару тобының жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. Саясатты таңдап, мәтінмәндік мәзір арқылы саясат сипаттары терезесіне өтіңіз.
4. Саясат сипаттары терезесінде **Саясат профильдері** бөлімін таңдап, **Қосылуда** түймесін басыңыз.

   Саясат профилін жасау шебері іске қосылады.
5. Шебердің **Саясат профилінің атауы** терезесінде келесіні көрсетіңіз:

   a. Саясат профилі атауы.

      Профиль атауы 100 таңбадан артық бола алмайды.

   b. Саясат профилінің күйі (*Қосулы* немесе *Өшірулі*).

      Белсенді емес саясат профильдерін құру ұсынылады және оларды саясат профильдерін іске қосу параметрлері мен шарттарын толығымен орнатқаннан кейін ғана қосу ұсынылады.
6. Жаңа саясат профилін белсендіру ережесін орнату шеберін іске қосу үшін **Саясат профилін жасау шеберін жапқаннан кейін, саясат профилін белсендіру ережесін конфигурациялауға өту** жалаушасын қойыңыз. Шебердің нұсқауларын орындаңыз.
7. Саясат профилінің сипаттары терезесінде саясат профилінің параметрлерін қажетінше өзгертіңіз.
8. **OK** түймесін басып, өзгерістерді сақтаңыз.

   Профиль сақталады. Профиль белсендіру ережелерін қанағаттандыратын құрылғыларда іске қосылады.

Бір саясат үшін бірнеше саясат профильдерін жасауға болады. Саясат үшін жасалған профильдер **Саясат профильдері** бөліміндегі саясат сипаттарында көрсетіледі. Саясат профилін және профиль басымдығын өзгерте аласыз, сондай-ақ профильді жоя аласыз.

Саясат профилін өзгерту

Саясат профилінің параметрлерін өзгерту

Профильді өзгерту тек Kaspersky Endpoint Security for Windows саясаттары үшін ғана қолжетімді.

Саясат профилін өзгерту үшін:

1. Консоль ағашында саясат профилін өзгерту үшін басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. Саясатты таңдап, мәтінмәндік мәзір арқылы саясат сипаттары терезесіне өтіңіз.
4. Саясат сипаттарында **Саясат профильдері** бөлімін ашыңыз.

   Бөлімде саясат үшін жасалған профильдердің тізімі берілген. Тізімдегі профильдер олардың басымдықтарына сәйкес көрсетіледі.
5. Саясат профилін таңдап, **Сипаттар** түймесін басыңыз.
6. Сипаттар терезесінде профиль параметрлерін конфигурациялаңыз:
   - Қажет болса, **Жалпы** бөлімінде профиль атауын өзгертіп, профильді **Профильді қосу** жалаушасы арқылы қосыңыз немесе өшіріңіз.
   - **Белсендіру ережелері** бөлімінде профильді белсендіру ережесін өңдеңіз.
   - Тиісті бөлімдердегі саясат параметрлерін өзгертіңіз.
7. **OK** түймесін басыңыз.

Өзгертілген параметрлер құрылғыны Басқару серверімен синхрондағаннан кейін (саясат профилі белсенді болса) немесе белсендіру ережесін орындағаннан кейін (саясат профилі белсенді болмаса) әрекет ете бастайды.

Саясат профилі басымдығын өзгерту

Саясат профильдерінің басымдығы клиент құрылғысындағы профильдерді белсендіру тәртібін анықтайды. Егер саясаттың әртүрлі профильдері үшін бірдей белсендіру ережелері берілсе, басымдық қолданылады.

Мысалы, екі саясат профилі қолданылса: бір-бірінен бір параметр мәндерімен (*Мән 1* және *Мән 2*) ерекшеленетін *Профиль 1* және *Профиль 2*. *Профиль 1* басымдығы *Профиль 2*-ден жоғары. Бұдан бөлек, басымдығы *Профиль 2*-ден де төмен профильдер бар. Профильді белсендіру ережелері сай келеді.

Белсендіру ережесін орындау кезінде *Профиль 1* белсендіріледі. Құрылғыдағы параметр *Мән 1* болып өзгертіледі. *Профиль 1*-ді жойсаңыз, онда *Профиль 2* басымдығы ең жоғары болып, параметр *Мән 2* болып өзгереді.

Саясат профильдерінің тізімінде профильдер олардың басымдықтарына сәйкес көрсетіледі. Тізімде бірінші орында басымдығы ең жоғары профиль тұр. Профиль басымдығын, жоғары көрсеткі  және төмен көрсеткі  түймелері арқылы өзгертуге болады.

Саясат профилін жою

Саясат профилін жою үшін:

1. Консоль ағашынан саясат профилін жою үшін басқару тобын таңдаңыз.
2. Басқару тобының жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. Саясатты таңдап, мәтінмәндік мәзір арқылы саясат сипаттары терезесіне өтіңіз.
4. Kaspersky Endpoint Security саясаты сипаттарында **Саясат профильдері** бөлімін ашыңыз.
5. Жойылатын саясат профилін таңдап, **Жою** түймесін басыңыз.

Нәтижесінде, саясат профилі жойылады. Белсендіру ережелері құрылғыда орындалатын басқа саясат профилі немесе саясат белсенді болады.

Саясатын профилін белсендіру ережесін жасау

Саясатын профилін белсендіру ережесін жасау үшін:

1. Консоль ағашында саясат профилін белсендіру ережесін жасау үшін басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. Саясатты таңдап, мәтінмәндік мәзір арқылы саясат сипаттары терезесіне өтіңіз.
4. Саясат сипаттары терезесінде **Саясат профильдері** бөлімін таңдаңыз.
5. Белсендіру ережесін жасау қажет болған саясат профилін таңдап, **Сипаттар** түймесін басыңыз.

   Нәтижесінде, саясат профилі сипаттары терезесі ашылады.

   Саясат профильдері тізімі бос болса, саясат профилін жасай аласыз.
6. **Белсендіру ережелері** бөлімін таңдап, **Қосылуда** түймесін басыңыз.

   Нәтижесінде, жаңа саясат профилін белсендіру ережесін орнату шебері іске қосылады.
7. **Саясат профилін белсендіру ережелері** терезесінде жасалғалы жатқан саясат профилін белсендіруге әсер етуі тиісті шарттарға қарама-қарсы жалаушалар қойыңыз:

   - **Саясат профилін белсендірудің жалпы ережелері**

     Құрылғының автономды режимі күйіне, құрылғыны Басқару серверіне қосу ережелеріне және құрылғыға тағайындалған тегтерге байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

- **Active Directory қызметін пайдалану ережелері**

  Құрылғының Active Directory бөлімшесінде орналасуына немесе құрылғының не оның иесінің Active Directory қауіпсіздік тобына мүше болуына байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

- **Арнайы құрылғының иесіне арналған ережелер**

  Құрылғының иесі кім екеніне және құрылғының Kaspersky Security Center ішкі қауіпсіздік тобына мүше болуына байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

- **Жабдық сипаттамалары ережелері**

  Жадтың көлеміне және құрылғының логикалық процессорларының санына байланысты құрылғыдағы саясатты белсендіру шартын конфигурациялау үшін жалаушаны қойыңыз.

Шебер терезелерінің кейінгі саны осы қадамдағы параметрлерді таңдауға байланысты. Саясат профилін белсендіру ережелерін кейінірек өзгертуге болады.

8. **Жалпы шарттар** бөлімінде келесі параметрлерді көрсетіңіз:

- **Құрылғы офлайн режимде** өрісінде, ашылатын тізімде құрылғыны желіде табу шартын көрсетіңіз:

  - **Иә**

    Құрылғы сыртқы желіде орналасқан, яғни Басқару сервері қолжетімді емес.

  - **Жоқ**

    Құрылғы желіде орналасқан, Басқару сервері қолжетімді.

  - **Мән таңдалмаған**

    Өлшемшарт қолданылмайды.

- **Құрылғы көрсетілген желілік орында орналасқан** өрісінде, ашылатын тізімдердің көмегімен құрылғыда Басқару серверіне қосылу ережесін орындаған/орындамаған кезде саясат профилін белсендіруді конфигурациялаңыз:

  - **Орындалуда/Орындалмауда**

    Саясат профилін белсендіру шарты (ереже орындалады немесе орындалмайды).

  - **Ереженің атауы**

    Шарттарын орындау немесе орындамау кезінде саясат профилі белсендірілетін Басқару серверіне қосылуға арналған құрылғының желілік орнының сипаттамасы.

    Басқару серверіне қосылу үшін құрылғылардың желілік орнының сипаттамасын Желілік агентті ауыстырып қосу ережесінде жасауға немесе конфигурациялауға болады.

Жалпы шарттар терезесі, **Саясат профилін белсендірудің жалпы ережелері** жалаушасы қойылған кезде көрсетіледі.

9. **Тегтер пайдаланылатын шарттар** бөлімінде келесі параметрлерді көрсетіңіз:

   - **Тегтер тізімі**

     Тегтер тізімінде қажетті тегтерге жалаушалар қою арқылы құрылғыларды саясат профиліне қосу ережесін белгілеңіз.

     Тізімге жаңа тегтерді қосу үшін оларды тізімнің үстіндегі өріске енгізіп, **Қосу** түймесін басуыңызға болады.

     Саясат профиліне, сипаттамасында барлық таңдалған тегтері бар құрылғылар қосылады. Жалаушалар алынып тасталса, өлшемшарт қолданылмайды. Әдепкі бойынша, жалаушалар алынып тасталған.

   - **Көрсетілген тегтерсіз құрылғыларға қолдану**

     Тег таңдауын терістету қажет болса, параметрді қосыңыз.

     Параметр қосулы болса, онда саясат профиліне, сипаттамасында таңдалған тегтері жоқ құрылғылар қосылады. Бұл параметр өшірулі болса, өлшемшарт қолданылмайды.

     Әдепкі бойынша, параметр өшірулі.

   Тегтер пайдаланылатын шарттар терезесі, **Саясат профилін белсендірудің жалпы ережелері** жалаушасы қойылған кезде көрсетіледі.

10. **Active Directory пайдаланылатын шарттар** бөлімінде келесі параметрлерді көрсетіңіз:

    - **Құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі**

      Параметр қосулы болса, онда саясат профилі, иесі аталған қауіпсіздік тобының мүшесі болып табылатын құрылғыда іске қосылады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

    - **Құрылғының Active Directory қауіпсіздік тобындағы мүшелігі**

      Параметр қосулы болса, құрылғыда саясат профилі белсендіріледі. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

    - **Active Directory бөлімшесіне құрылғыны орналастыру**

      Параметр қосулы болса, саясат профилі көрсетілген Active Directory бөлімшесіне кіретін құрылғыда белсендіріледі. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды.

      Әдепкі бойынша, параметр өшірулі.

    Active Directory пайдаланылатын шарттар терезесі, **Active Directory қызметін пайдалану ережелері** жалаушасы қойылған кезде көрсетіледі.

11. **Құрылғы иесі пайдаланылатын шарттар** бөлімінде келесі параметрлерді көрсетіңіз:

- **Құрылғының иесі**

  Құрылғының иесі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғы көрсетілген иеленушіге тисілі ("=" белгісі);
  - құрылғы көрсетілген иеленушіге тисілі емес ("#" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Параметр қосылған кезде, құрылғы иесін көрсетуіңізге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Құрылғы иесі ішкі қауіпсіздік тобына кіреді**

  Kaspersky Security Center ішкі қауіпсіздік тобындағы құрылғы иесінің мүшелігі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғының иесі көрсетілген қауіпсіздік тобының мүшесі ("=" белгісі);
  - құрылғының иесі көрсетілген қауіпсіздік тобының мүшесі емес ("#" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Сіз Kaspersky Security Center қауіпсіздік тобын көрсете аласыз. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Құрылғы иесінің арнайы рөлі бойынша саясат профилін белсендіру**

  Құрылғы иесінің белгілі бір рөлінің болуына байланысты, құрылғыда саясат профилін белсендіру ережесін конфигурациялау және қосу үшін осы параметрді қосыңыз. Қолданыстағы рөлдер тізімінен рөлді қолмен қосыңыз.

  Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады.

Құрылғы иесі пайдаланылатын шарттар терезесі, **Арнайы құрылғының иесіне арналған ережелер** жалаушасы қойылған кезде көрсетіледі.

12. **Жабдық сипаттамалары пайдаланылатын шарттар** бөлімінде келесі параметрлерді көрсетіңіз:

- **Жедел жадтың көлемі, МБ түрінде**

  Құрылғының жедел жад көлемі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғының жедел жады көлемі көрсетілген мәннен аз ("<" белгісі);
  - құрылғының жедел жады көлемі көрсетілген мәннен артық (">" белгісі).

  Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Құрылғының жедел жадының көлемін көрсетуге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Логикалық процессорлардың саны**

  Құрылғының логикалық процессорлардың саны бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғының логикалық процессорларының саны көрсетілген мәннен аз немесе оған тең ("<" белгісі);
  - құрылғының логикалық процессорларының саны көрсетілген мәннен артық немесе оған тең (">" белгісі).

  Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Құрылғының логикалық процессорларының санын көрсетуіңізге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

Жабдық сипаттамалары пайдаланылатын шарттар терезесі, **Жабдық сипаттамалары ережелері** жалаушасы қойылған кезде көрсетіледі.

13. **Саясат профилін белсендіру ережесінің аты** терезесінде, **Ереженің атауы** өрісінде ереженің атауын көрсетіңіз.

Нәтижесінде, профиль сақталады. Белсендіру ережелері орындалған кезде профиль құрылғыда белсендіріледі.

Профиль үшін жасалған саясат профилін белсендіру ережелері **Белсендіру ережелері** бөліміндегі саясат профилінің сипаттарында көрсетіледі. Саясат профилін белсендіру ережесін өзгертуге немесе жоюға болады.

Бірнеше белсендіру ережесі бір уақытта орындалуы мүмкін.

Құрылғыны жылжыту ережелері

Құрылғыларды жылжыту ережелері көмегімен басқару топтарында құрылғыларды орналастыру процесін автоматтандыру ұсынылады. Жылжыту ережесі үш негізгі бөліктен тұрады: атауы, орындау шарттары (құрылғы атрибуттарының логикалық өрнегі) және мақсатты басқару тобы. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда ереже құрылғыны мақсатты басқару тобына көшіреді.

Құрылғыны жылжыту ережелерінің басымдықтары бар. Басқару сервері құрылғының атрибуттарын әрбір ережені орындау шартына сай келу тұрғысынан, ережелер басымдығының азаюы тәртібінде тексереді. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда құрылғы мақсатты топқа көшіріледі және бұл құрылғы үшін ережелерді өңдеу осымен тоқтайды. Егер құрылғының атрибуттары бірден бірнеше ережеге сай келсе, онда құрылғы үлкен басымдыққа ие ереженің мақсатты тобына көшіріледі (ережелер тізімінде жоғары тұр).

Құрылғыны жылжыту ережелері айқын емес түрде жасалуы мүмкін. Мысалы, қашықтан орнату тапсырмасының немесе пакетінің сипаттарында, Желілік агентті орнатқаннан кейін құрылғы кіруі тиісті басқару тобы көрсетілуі мүмкін. Сондай-ақ, жылжыту ережелерін Kaspersky Security Center әкімшісі айқын түрде, жылжыту ережелерінің тізімінде жасай алады. Тізім **Тағайындалмаған құрылғылар** топ сипаттарындағы Басқару консолінде орналасқан.

Жылжыту ережесі, әдепкі бойынша құрылғыларды басқару топтарында бір рет бастапқы орналастыруға арналған. Ереже **Тағайындалмаған құрылғылар** тобында орналасқан құрылғыларды тек қана бір рет жылжытады. Егер құрылғы бір жолы осы ережемен жылжытылса, құрылғыны қолмен **Тағайындалмаған құрылғылар** тобына қайтарса да, ереже оны қайтадан жылжытпайды. Бұл, жылжыту ережелерін қолданудың ұсынылатын тәсілі.

Басқару топтарында әлдеқашан орналастырылған құрылғыларды жылжытуға болады. Бұл үшін ереже сипаттарында **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту** жалаушасын алып тастаңыз.

Басқару топтарында әлдеқашан орналастырылған құрылғыларға қолданылатын жылжыту ережелерінің болуы, Басқару серверіне түсетін жүктемені едәуір арттырады.

Тек басқару тобында орналастырылмаған құрылғыларды жылжыту жалаушасы автоматты түрде жасалған жылжыту ережелерінің сипаттарында бұғатталған. Мұндай ережелер *Бағдарламаларды қашықтан орнату* тапсырмасын қосқанда немесе автономды орнату пакетін жасағанда құрылады.

Бір құрылғыда көп рет әрекет ете алатын жылжыту ережесін жасауға болады.

Бір құрылғы топтан топқа көп рет жылжыту, мысалы, құрылғыға арнайы саясатты қолдану, арнайы топтық тапсырманы іске қосу, белгілі бір тарату нүктесінен жаңарту мақсатында басқарылатын құрылғылармен жұмыс істеу тәсілдемесінен аулақ болу қатаң ұсынылады.

Мұндай сценарийлерге қолдау көрсетілмейді, өйткені олар Басқару серверіне және желілік трафикке жүктеу бойынша онша тиімсіз. Сондай-ақ, бұл сценарийлер Kaspersky Security Center жұмыс моделіне қарама-қайшы келеді (әсіресе, қатынасу құқықтары, оқиғалар мен есептер саласында). Басқа шешім іздеу, мысалы, саясат профильдерін, құрылғыларды таңдауға арналған тапсырмаларды қолдану, әдістемеге сәйкес желілік агенттерді тағайындау керек.

Құрылғыны жылжыту ережелерін көшіру

Егер сізге ұқсас параметрлері бар бірнеше құрылғыны жылжыту ережелерін жасау қажет болса, қолданыстағы ережені көшіріп, содан кейін көшірілген ереженің параметрлерін өзгертуге болады. Мысалы, әртүрлі IP ауқымдары мен мақсатты топтары бар бірнеше бірдей құрылғыны жылжыту ережелері болуы керек болған кезде ыңғайлы.

Құрылғыны жылжыту ережесін көшіру үшін:

1. Бағдарламаның басты терезесін ашыңыз.
2. **Тағайындалмаған құрылғылар** қалтасында **Ережелерді конфигурациялау** түймесін басыңыз.

   Сипаттар: Тағайындалмаған құрылғылар терезесі ашылады.
3. **Құрылғыларды жылжыту** бөлімінде, көшіргіңіз келетін құрылғыларды жылжыту ережесін таңдаңыз.
4. **Клон ережесі** түймесін басыңыз.

   Таңдалған ереженің көшірмесі тізімнің соңына қосылады.

Жаңа ереже өшірулі болып жасалады. Ережені кез келген уақытта өшіруге немесе өзгертуге болады.

Бағдарламалық жасақтаманы санаттау

Қолданбаларды іске қосуды бақылаудың негізгі құралы *Kaspersky* санаттары болып табылады (бұдан әрі *KL санаттар*). KL санаты Kaspersky Security Center әкімшісіне БЖ категориялауды қолдау жұмысын жеңілдетеді және басқарылатын құрылғыларға жіберілетін трафик көлемін барынша азайтады.

Реттелмелі санаттарды бірде-бір KL санатқа түспейтін бағдарламалар үшін ғана жасау керек (мысалы, тапсырысқа әзірленген бағдарламалар үшін). Реттелмелі санаттар бағдарламаның дистрибутиві (MSI) негізінде немесе дистрибутивтері бар қалтаның негізінде жасалады.

Егер KL санаттармен категорияланбаған бағдарламалық жасақтаманың үлкен толықтырылатын топтамасы болса, автоматты түрде жаңартылатын санатты жасаған жөн. Мұндай санат автоматты түрде дистрибутивтері бар қалтаны өзгерту кезінде орындалатын файлдардың бақылау сомаларымен толықтырылады.

Менің құжаттарым, %windir%, %ProgramFiles% және %ProgramFiles(x86)% қалталары үшін автоматты түрде жаңартылған бағдарламалық жасақтама санаттарын жасамаңыз. Бұл қалталардағы файлдар жиі өзгереді, бұл Басқару серверіне жүктемені ұлғайтуға және желідегі трафикті ұлғайтуға әкеледі. Бағдарламалық жасақтаманың топтамасы бар бөлек қалта жасау және оны кейде толықтыру керек.

Бағдарламаларды ұйым-клиент құрылғыларына орнату үшін қажетті шарттар

Ұйым-клиенттің құрылғыларына бағдарламаларды қашықтан орнату процесі ұйым ішіндегі бағдарламаларды қашықтан орнату процесіне сәйкес келеді.

Ұйым-клиенттің құрылғыларына бағдарламаларды орнату үшін келесі шарттарды орындау қажет:

- Ұйым-клиенттің құрылғыларына бағдарламаларды бірінші рет орнатудың алдында, оларға Желілік агент орнату қажет.

  Kaspersky Security Center бағдарламасында провайдердің Желілік агентінің орнату пакетін орнату кезінде орнату пакетінің сипаттары терезесінде келесі параметрлерді конфигурациялау қажет:

  - **Қосылым** бөлімінде **Басқару сервері** жолында Желілік агентті тарату нүктесіне жергілікті орнатқан кездегідей виртуалды Басқару серверінің мекенжайын көрсету қажет.

  - **Кеңейтілген** бөлімінде **Басқару серверіне байланыс шлюзі арқылы қосылу** жалаушасын қойыңыз. **Қосылым шлюзінің мекенжайы** жолында тарату нүктесінің мекенжайын көрсету керек. Құрылғының мекенжайы ретінде Windows желісіндегі IP мекенжайын немесе құрылғының атауын пайдалануға болады.

- Желілік агенттің орнату пакетін жүктеу тәсілі ретінде **Тарату нүктелерінің көмегімен операциялық жүйенің құралдарымен** тармағын таңдау керек. Жүктеу тәсілі келесідей таңдалады:
  - Бағдарламаларды қашықтан орнату тапсырмаларын пайдаланып орнатқан кезде жүктеу тәсілін екі жолмен таңдауға болады:
    - **Параметрлер** терезесінде қашықтан орнату тапсырмасын жасау кезінде;
    - **Параметрлер** бөлімінде қашықтан орнату тапсырмасы сипаттары терезесінде.
  - Бағдарламаларды қашықтан орнату шебері арқылы орнатқан кезде жүктеу тәсілін **Параметрлер** шебері терезесінде таңдауға болады.
- Тарату нүктесі жұмыс істейтін есептік жазба клиент құрылғыларындағы Admin$ ресурсына қатынаса алуы керек.

Бағдарламаның жергілікті параметрлерін көру және өзгерту

Kaspersky Security Center Басқару жүйесі құрылғылардағы бағдарламалардың жергілікті параметрлерін Басқару консолі арқылы қашықтан басқаруға мүмкіндік береді.

Бағдарламаның жергілікті параметрлері – құрылғыға тән бағдарлама параметрлері. Kaspersky Security Center көмегімен басқару топтарына кіретін құрылғылар үшін бағдарламаның жергілікті параметрлерін орнатуға болады.

Kaspersky бағдарламаларының параметрлерінің егжей-тегжейлі сипаттамасы осы бағдарламаларға арналған нұсқаулықтарда келтірілген.

Бағдарламаның жергілікті параметрлерін көру немесе өзгерту үшін:

1. Қажетті құрылғыны қамтитын топтың жұмыс аймағында **Құрылғылар** қойыншасын таңдаңыз.
2. Сипаттар терезесінде **Бағдарламалар** бөлімінде тиісті бағдарламаны таңдаңыз.
3. Бағдарлама атауын екі рет басу немесе **Сипаттар** түймесін басу арқылы бағдарлама сипаттары терезесін ашыңыз.

Нәтижесінде, таңдалған бағдарламаның жергілікті параметрлері терезесі пайда болады, оны көруге және өзгертуге болады.

Топтық саясатта өзгертуге тыйым салынбаған параметрлердің мәндерін өзгертуге болады (параметр саясатта (🔒) құлыпталған).

Kaspersky Security Center және басқарылатын бағдарламаларды жаңарту

Бұл бөлімде Kaspersky Security Center және басқарылатын бағдарламаларды жаңарту үшін орындалатын қадамдар сипатталған.

Сценарий: Kaspersky бағдарламалары мен дерекқорларын үнемі жаңартып тұру

Бұл бөлімде Kaspersky дерекқорлары, бағдарламалық модульдері мен бағдарламаларын үнемі жаңартып тұру сценарийі ұсынылған. Сіз Ұйымның желісінде қорғаныспен конфигурациялау сценарийін аяқтағаннан кейін, Басқару серверлері мен басқарылатын құрылғыларды түрлі қауіптерден, сонымен қатар вирустардан, желілік шабуылдардан және фишингтік шабуылдардан қорғауды қамтамасыз ету үшін қорғаныс жүйесінің сенімділігін қамтамасыз етуге тиіссіз.

Желі қорғанысына, келесіні үнемі жаңартып тұру арқылы қолдау көрсетіледі:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;
- Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

Сіз осы сценарийді аяқтағаннан кейін, келесіге сенімді бола аласыз:

- Сіздің желіңіз Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky ең соңғы бағдарламалық жасақтамасымен қорғалған.
- Желі қауіпсіздігі үшін критикалық тұрғыдан маңызды болып саналатын Kaspersky антивирустық дерекқорлары мен басқа да дерекқорлары, әрдайым өзекті.

Алдын ала талаптар

Басқарылатын құрылғылардың Басқару серверімен қосылымы болуы тиіс. Құрылғылардың қосылымы болмаса, Kaspersky дерекқорлары, бағдарламалық модульдері мен бағдарламаларын қолмен немесе тікелей Kaspersky жаңарту серверлерінен жаңарту мүмкіндігін қарастырып көріңіз.

Басқару серверінің интернетке қосылымы болуы тиіс.

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

1. Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалық жасақтамасын орналастыру сценарийіне сәйкес басқарылатын құрылғыларда Kaspersky қауіпсіздік бағдарламалары орналастырылды.
2. Желі қорғанысын конфигурациялау сценарийіне сәйкес барлық қажетті саясаттар, саясат профильдері және тапсырмалар жасалған және конфигурацияланған.
3. Басқарылатын құрылғылардың санына және желі топологиясына сәйкес тарату нүктелерінің тиісті саны тағайындалған.

Kaspersky бағдарламалары мен дерекқорларын жаңарту келесі кезеңдерден тұрады:

1. **Жаңарту схемасын таңдау**

   Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларының жаңартуларын орнату үшін қолдануға болатын бірнеше схема бар. Желіңіздің талаптарына бәрінен жақсы сай келетін схеманы немесе бірнеше схеманы таңдап алыңыз.

2 Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау

Бұл тапсырма Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы дәл қазір жасаңыз.

Бұл тапсырма жаңартуларды Kaspersky жаңартулар серверлерінен Басқару сервері қоймасына, сондай-ақ Kaspersky Security Center үшін дерекқорлар мен бағдарламалық модульдердің жаңартуларын жүктеп алуға қажет. Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

Сіздің желіңізде тарату нүктелері тағайындалған болса, жаңартулар Басқару серверінің қоймасынан тарату нүктелерінің қоймаларына автоматты түрде жүктеледі. Бұл жағдайда, тарату нүктесінің ауқымына кіретін басқарылатын құрылғылар Басқару серверінің қоймасы орнына жаңартуларды тарату нүктелерінің қоймаларынан жүктеп алады.

Нұсқаулар:

- Басқару консолі: Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау.
- Kaspersky Security Center Web Console: Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау.

3 Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау (қажет болса)

Әдепкі бойынша, жаңартулар Басқару сервері қоймасынан тарату нүктелерінің қоймаларына жүктеледі. Сіз Kaspersky Security Center бағдарламасын, тарату нүктелері жаңартуларды тікелей Kaspersky жаңарту серверлерінен жүктейтін етіп конфигурациялай аласыз. Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса, жаңартулары тарату нүктелерінің қоймаларынан жүктеп алу артық көрінеді.

Сіздің желіңізге тарату нүктелері тағайындалып, *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы жасалған кезде, тарату нүктелері жаңартуларды Басқару сервері қоймасынан емес, Kaspersky жаңарту серверлерінен жүктейді.

Нұсқаулар:

- Басқару консолі: Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау.
- Kaspersky Security Center Web Console: Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау.

4 Тарату нүктелерін конфигурациялау

Сіздің желіңізге тарату нүктелері тағайындалған болса, **Жаңартуларды тарату** параметрі барлық қажетті тарату нүктелеріндегі сипаттарда қосылғанына көз жеткізіңіз. Егер бұл параметр тарату нүктесі үшін өшірулі болса, тарату нүктесінің ауқымына қосылған құрылғылар Басқару сервері қоймасынан жаңартуларды жүктейді.

Егер сіз басқарылатын құрылғылардың тек тарату нүктелерінен жаңартулар алуын қаласаңыз, Желілік агент саясатындағы **Файлдарды тек тарату нүктелері арқылы тарату** параметрін қосыңыз.

5 Жаңартуларды алудың немесе айырмашылық файлдарын жүктеудің офлайн моделін қолдана отырып, жаңарту процесін оңтайландыру (қажет болса)

Жаңарту процесін, жаңартуларды жүктеудің офлайн моделін (әдепкі бойынша қосылған) немесе айырмашылық файлдарын пайдалану арқылы оңтайландыруға болады Әрбір желі сегменті үшін осы екі функцияның қайсысын қосу керектігін таңдау керек, өйткені олар бір уақытта жұмыс істей алмайды.

Жаңартуларды алудың офлайн моделі қосылған кезде, қауіпсіздік бағдарламасы жаңартуларды сұрамас бұрын, Желілік агент жаңартуларды Басқару сервері қоймасына жүктегеннен кейін басқарылатын құрылғыға қажетті жаңартуларды жүктейді. Бұл жаңарту процесінің сенімділігін арттырады. Бұл функцияны пайдалану үшін Желілік агент саясаты тапсырмасының сипаттарындағы **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)** параметрін қосыңыз.

Егер сіз жаңартуларды жүктеудің офлайн моделін пайдаланбасаңыз, айырмашылық файлдарын қолдана отырып, Басқару сервері мен басқарылатын құрылғылар арасындағы трафикті оңтайландыруға болады. Бұл функция қосылған кезде, Басқару сервері немесе тарату нүктесі Kaspersky бүкіл дерекқор файлдарының немесе бағдарламалық модульдерінің орнына айырмашылық файлдарын жүктейді. Айырмашылықтар файлы дерекқор немесе бағдарламалық модуль файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Сондықтан, айырмашылық файлдары бүкіл файлдарға қарағанда аз орын алады. Нәтижесінде, Басқару сервері немесе тарату нүктелері және басқарылатын құрылғылар арасындағы трафик азаяды. Бұл функцияны пайдалану үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* және/немесе *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының сипаттарындағы **diff файлдарды жүктеп алу** параметрін қосыңыз.

Нұсқаулар:

- Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану.
- Басқару консолі: Жаңартуларды алудың офлайн-моделін қосу және өшіру.
- Kaspersky Security Center Web Console: Басқару консолі: Жаңартуларды алудың офлайн моделін қосу және өшіру.

6 Алынған жаңартуларды тексеру (қажет болса)

Жүктелген жаңартуларды орнатпас бұрын, *Жаңартуларды тексеру* тапсырмасын пайдаланып, жаңартуларды тексеруге болады. Бұл тапсырма құрылғыны жаңарту тапсырмаларын және аталған сынақ құрылғыларының жиынтығына арналған параметрлермен конфигурацияланған зиянды БҚ іздеу тапсырмаларын дәйекті түрде іске қосады. Тапсырма нәтижелерін алғаннан кейін, Басқару сервері жаңартуларды қалған құрылғыларға таратуды бастайды немесе бұғаттайды.

Жаңартуларды тексеру тапсырмасы *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының бөлігі ретінде орындалуы мүмкін. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы сипаттарында, Басқару консолінде **Тарату алдында жаңартулар бар-жоғын тексеруді орындау** параметрін немесе Kaspersky Security Center Web Console веб-консолінде **Жаңарту тексерісін іске қосу** параметрін қосыңыз.

Нұсқаулар:

- Басқару консолі: Алынған жаңартуларды тексеру.
- Kaspersky Security Center Web Console: Алынған жаңартуларды тексеру.

7 Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау

Әдепкі бойынша, жүктелген бағдарламалық жасақтама жаңартулары *Анықталмаған* күйіне ие. Жаңарту күйін *Расталды* немесе *Қабылданбады* күйіне өзгертуге болады. Бекітілген жаңартулар әрқашан орнатылады. Егер жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдауыңыз қажет. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін. Анықталмаған жаңартуларды тек Желілік агентке және Kaspersky Security Center басқа құрамдастарына Желілік агент саясатының параметрлеріне сәйкес орнатуға болады. Сіз *Қабылданбады* деп белгілеген жаңартулар, басқарылатын құрылғыларға орнатылмайды. Егер қауіпсіздік бағдарламасы үшін бұрын қабылданбаған жаңарту орнатылған болса, Kaspersky Security Center барлық бағдарламасы құрылғылардан жаңартуларды жоюға тырысады.

Жаңартуларды мақұлдау және қабылдамау Windows операциялық жүйесімен жұмыс істейтін клиент құрылғыларына орнатылған желілік агент пен Kaspersky басқарылатын қолданбалары үшін ғана қолжетімді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
- Kaspersky Security Center Web Console: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау.

8. **Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнатуды конфигурациялау**

   Желілік агентке және Kaspersky Security Center басқа құрамдастарына жүктелген жаңартулар мен патчтар автоматты түрде орнатылады. Егер сіз Желілік агенттің сипаттарында **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату** параметрін қосулы қалдырсаңыз, онда барлық жаңартулар қоймаға (немесе бірнеше қоймаға) жүктелгеннен кейін автоматты түрде орнатылады. Егер жалауша алынып тасталса, *Анықталмаған* мәртебесі бар Kaspersky жүктелген патчтары, әкімші олардың мәртебесін *Расталды* деп өзгерткеннен кейін орнатылады.

   Нұсқаулар:

   - Басқару консолі: Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру.
   - Kaspersky Security Center Web Console: Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру.

9. **Басқару сервері үшін жаңартуларды орнату**

   Басқару серверіне арналған бағдарламалық жасақтама жаңартулары жаңарту күйлеріне тәуелді емес. Олар автоматты түрде орнатылмайды және Басқару консоліндегі **Мониторинг** қойыншасында (**Басқару сервері** `<Сервер атауы>` → **Мониторинг**) немесе Kaspersky Security Center Web Console веб-консоліндегі **Хабарландырулар** бөлімінде (**Бақылау және есеп беру** → **Хабарландырулар**) әкімші тарапынан алдын ала мақұлдануы тиіс. Осыдан кейін, әкімші жаңартуларды орнатуды нақты түрде бастауы керек.

10. **Қауіпсіздік бағдарламалары үшін жаңартуларды автоматты түрде орнатуды конфигурациялау**

    Kaspersky бағдарламаларын, бағдарламалық модульдерін және дерекқорларын, соның ішінде антивирустық базаларды уақтылы жаңартуды қамтамасыз ету мақсатында, басқарылатын бағдарламалар үшін *Жаңарту* тапсырмасын жасаңыз. Уақтылы жаңарту үшін тапсырмалар кестесін конфигурациялау кезінде **Қоймаға жаңартуларды жүктеу кезінде** параметрін таңдау ұсынылады.

    Егер сіздің желіңізде тек IPv6 қолдайтын құрылғылар болса және сіз осы құрылғыларда орнатылған қауіпсіздік бағдарламаларын үнемі жаңартып отырғыңыз келсе, басқарылатын құрылғыларда Басқару сервері (13.2 немесе одан жоғары нұсқалар) және Желілік агент (13.2 немесе одан жоғары нұсқалар) орнатылғанына көз жеткізіңіз.

    Әдепкі бойынша, Kaspersky Endpoint Security for Windows және Kaspersky Endpoint Security for Linux үшін жаңартулар тек жаңарту күйі *Расталды* болып өзгертілгеннен кейін ғана орнатылады. *Жаңарту* тапсырмасында жаңарту параметрлерін өзгертуге болады.

    Егер жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдауыңыз қажет. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін.

    Нұсқаулар:

    - Басқару консолі: Құрылғыларға Kaspersky Endpoint Security жаңартуларын автоматты түрде орнату.
    - Kaspersky Security Center Web Console: Басқару консолі: Құрылғыларға Kaspersky Endpoint Security жаңартуларын автоматты түрде орнату.

Нәтижелер

Сценарий аяқталғаннан кейін, Kaspersky Security Center бағдарламасы Басқару сервері қоймасына немесе тарату нүктелерінің қоймаларына жаңартуларды жүктегеннен кейін, Kaspersky дерекқорларын және Kaspersky орнатылған бағдарламаларын жаңартуға арналған. Енді сіз желі жұмысын бақылауға кірісе аласыз.

Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту туралы

Басқару серверлері мен басқарылатын құрылғыларды қорғау жаңартылған күйде екеніне көз жеткізу үшін келесі жаңартуларды уақтылы ұсыну керек:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;

  Kaspersky Security Center бағдарламасы Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктемес бұрын Kaspersky серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Бұл антивирустық дерекқорларды жаңарту және басқарылатын құрылғылардың қауіпсіздік деңгейін сақтау үшін қажет.

- Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

  Kaspersky Security Center сізге Windows жүйесімен жұмыс істейтін клиенттік құрылғыларда орнатылған Желілік агент пен Kaspersky қолданбаларын автоматты түрде жаңартуға мүмкіндік береді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді. Бұл компоненттерді жаңарту үшін, олардың соңғы нұсқаларын Kaspersky сайтынан жүктеп алу және қолмен орнату керек.

Желіңіздің конфигурациясына байланысты сіз келесі жүктеу схемаларын қолдана аласыз және басқарылатын құрылғыларға қажетті жаңартуларды тарата аласыз:

- Бір тапсырмамен: *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*
- Екі тапсырманың көмегімен:
  - *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмалары.
  - *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмалары.
- Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен
- Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін Kaspersky жаңарту серверлерінен тікелей
- Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын пайдалану

Бұл схемада Kaspersky Security Center жаңартуларды *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы арқылы жүктейді. Желінің бір сегментінде 300-ден аз басқарылатын құрылғы немесе әр сегментте оннан аз басқарылатын құрылғы бар шағын желілерде, жаңартулар басқарылатын құрылғыларға тікелей Басқару серверінің қоймасынан таралады (төмендегі суретті қараңыз).

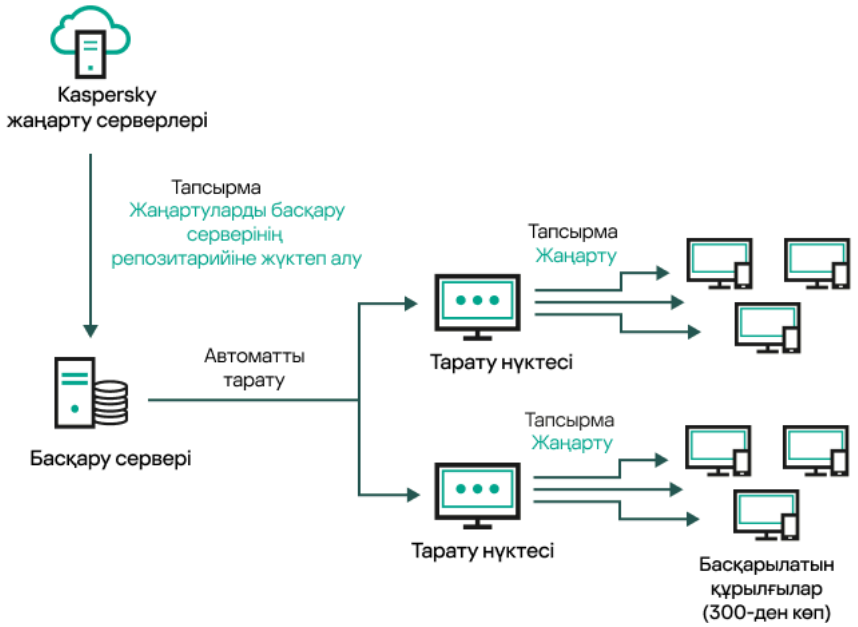


Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолдану арқылы және тарату нүктелерінсіз жаңарту

Әдепкі бойынша, Басқару сервері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Егер сіздің желіңізде бір желі сегментінде 300-ден астам басқарылатын құрылғы болса немесе сіздің желіңізде тоғыздан астам басқарылатын құрылғысы бар бірнеше сегмент болса, жаңартуларды басқарылатын құрылғыларға тарату үшін тарату нүктелерін пайдалануды ұсынамыз (төмендегі суретті қараңыз). Тарату нүктелері Басқару серверіне түсетін жүктемені азайтады және Басқару сервері мен басқарылатын құрылғылар арасындағы трафикті оңтайландырады. Тарату нүктелерінің санын және олардың желіңізге қажетті конфигурациясын есептеуіңізге болады.

Бұл схемада жаңартулар Басқару сервері қоймасынан тарату нүктесінің қоймаларына автоматты түрде жүктеледі. Тарату нүктесінің ауқымына кіретін басқарылатын құрылғылар Басқару серверінің қоймасы орнына жаңартуларды тарату нүктелерінің қоймаларынан жүктеп алады.



Тарату нүктелері бар Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолдану арқылы жаңарту

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы аяқталғаннан кейін, келесі жаңартулар Басқару серверінің қоймасына жүктеледі:

- Kaspersky Security Center үшін Kaspersky дерекқорлары мен бағдарламалық модульдері.

  Бұл жаңартулар автоматты түрде орнатылады.

- Басқарылатын құрылғылардағы қауіпсіздік бағдарламаларына арналған Kaspersky дерекқорлары мен бағдарламалық модульдері.

  Бұл жаңартулар Kaspersky Endpoint Security for Windows жаңарту тапсырмасы арқылы орнатылады.

- Басқару серверіне арналған жаңартулар.

  Бұл жаңартулар автоматты түрде орнатылмайды. Әкімші жаңартуларды нақты мақұлдап, жаңартуларды орнатуды іске қосуы керек.

  > Басқару серверіне патчтарды орнату үшін жергілікті әкімші құқықтары қажет.

- Kaspersky Security Center құрамдастарына арналған жаңартулар.

  Әдепкі бойынша, бұл жаңартулар автоматты түрде орнатылады. Сіз Желілік агент саясатының параметрлерін өзгерте аласыз.

- Қауіпсіздік бағдарламаларына арналған жаңартулар.

  Әдепкі бойынша, Kaspersky Endpoint Security for Windows бағдарламасы сіз мақұлдаған жаңартуларды ғана орнатады. (Сіз Басқару консолі немесе Kaspersky Security Center Web Console арқылы жаңартуларды мақұлдай аласыз). Жаңартулар *Жаңарту* тапсырмасы арқылы орнатылады және сол тапсырманың сипаттарында конфигурациялануы мүмкін.

> *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы жүктеп алу тапсырмасы виртуалды Басқару серверлерінде қолжетімді емес. Виртуалды сервердің қоймасы негізгі Басқару серверіне жүктелген жаңартуларды көрсетеді.

Алынған жаңартуларды жұмысқа жарамдылық тұрғысынан және сынақ құрылғыларының жиынтығында қателердің болуы тұрғысынан тексеруге конфигурациялауға болады. Егер тексеру сәтті болса, жаңартулар басқа басқарылатын құрылғыларға таралады.

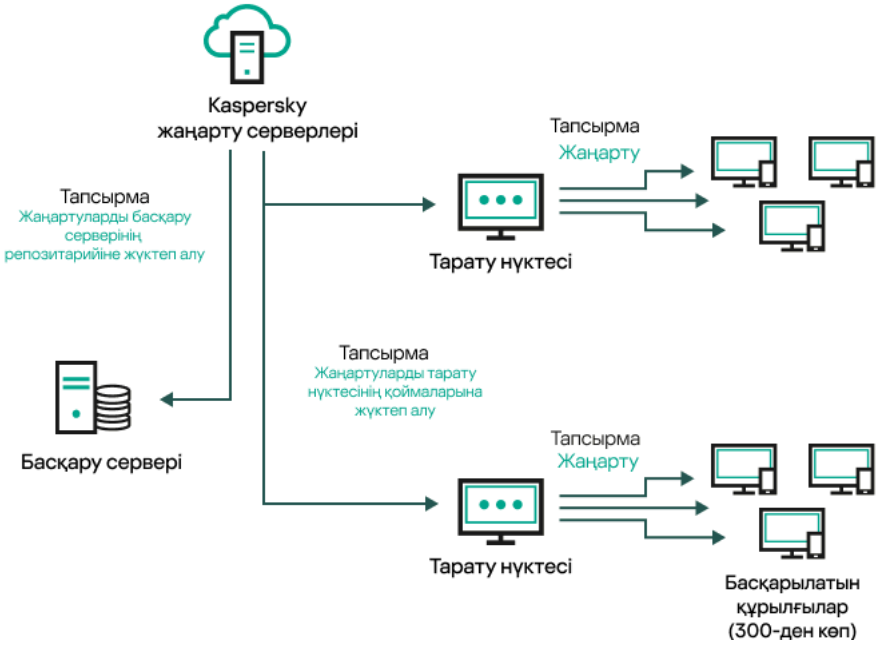
Әрбір басқарылатын Kaspersky бағдарламасы Басқару серверінен қажетті жаңартуларды сұрайды. Басқару сервері осы сұрауларды біріктіреді және тек бағдарламалар сұрайтын жаңартуларды жүктейді. Осылайша, тек қажетті жаңартулар және тек бір рет қана жүктелетіні қамтамасыз етіледі. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын орындау кезінде Kaspersky дерекқорлары мен бағдарламалық модульдерінің қажетті нұсқаларының жүктелуін қамтамасыз ету үшін Kaspersky жаңарту серверлеріне автоматты түрде Басқару сервері мынадай ақпаратты жібереді:

- Бағдарламаның идентификаторы және нұсқасы
- Қолданбаны орнату идентификаторы
- Белсенді кілт идентификаторы
- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын іске қосу идентификаторы

Берілетін ақпарат дербес деректерді және басқа да құпия деректерді қамтымайды. АО "Лаборатория Касперского" алынған ақпаратты заңда белгіленген талаптарға сәйкес қорғайды.

Екі тапсырманы пайдалану: Жаңартуларды Басқару серверінің қоймасына жүктеп алу және Жаңартуларды тарату орындарының қоймаларына жүктеп алу

Тарату нүктелерінің қоймаларына жаңартуларды Басқару сервері қоймасының орнына тікелей Kaspersky жаңарту серверлерінен жүктеп алуға болады, содан кейін жаңартуларды басқарылатын құрылғыларға таратуға болады (төмендегі суретті қараңыз). Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса, жаңартулары тарату нүктелерінің қоймаларынан жүктеп алу артық көрінеді.



Жаңартуларды Басқару серверінің қоймасына жүктеп алу және Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмалары көмегімен жаңарту

Әдепкі бойынша, Басқару сервері мен тарату нүктелері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін және/немесе тарату нүктелерін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Бұл схеманы іске асыру үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасына қосымша ретінде *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын жасаңыз. Осыдан кейін, тарату нүктелері жаңартуларды Басқару серверінің қоймасынан емес, Kaspersky жаңарту серверлерінен жүктейді.

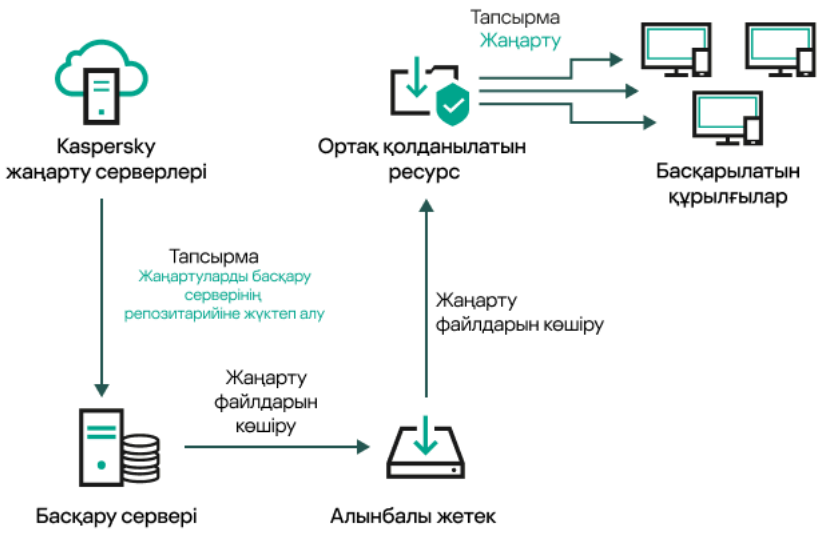
macOS басқаруындағы тарату нүктелері Kaspersky жаңарту серверлерінен жаңартуларды жүктеп ала алмайды.

macOS операциялық жүйесі бар құрылғылар *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының әрекет ету ауқымында болса, онда тапсырма Windows операциялық жүйесі бар құрылғылардың барлығында сәтті аяқталса да, *Сәтсіз аяқталды* мәртебесімен аяқталады.

Бұл схема үшін де *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы керек, себебі бұл тапсырма Kaspersky Security Center үшін Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктеу үшін қолданылады.

Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен

Егер клиент құрылғылары Басқару серверіне қосылмаған болса, сіз жергілікті қалтаны немесе ортақ ресурсты Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту көзі ретінде пайдалана аласыз. Бұл схемада қажетті жаңартуларды Басқару сервері қоймасынан алынбалы дискіге көшіру керек, содан кейін жаңартуларды жергілікті қалтаға немесе Kaspersky Endpoint Security параметрлерінде жаңарту көзі ретінде көрсетілген ортақ ресурсқа көшіру керек (төмендегі суретті қараңыз).



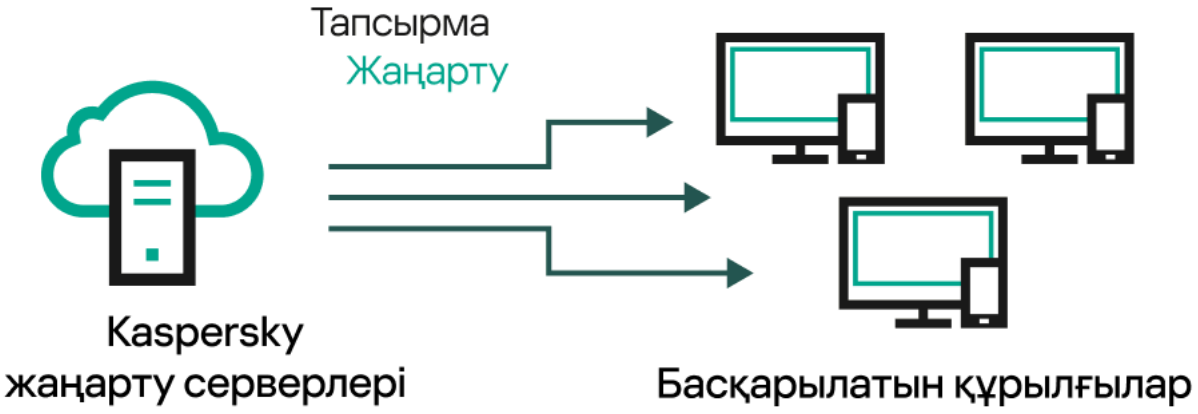
Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы жаңарту

Kaspersky Endpoint Security бағдарламасындағы жаңарту көздері туралы қосымша ақпарат алу үшін келесі анықтамаларды қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы

Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін Kaspersky жаңарту серверлерінен тікелей

Басқарылатын құрылғыларда сіз Kaspersky Endpoint Security бағдарламасын Kaspersky жаңарту серверлерінен тікелей жаңартуларды алу үшін конфигурациялай аласыз (төмендегі суретті қараңыз).



Қауіпсіздік бағдарламаларын тікелей Kaspersky жаңарту серверлерінен жаңарту

Бұл схемада қауіпсіздік бағдарламалары Kaspersky Security Center ұсынған қоймаларды пайдаланбайды. Жаңартуларды тікелей Kaspersky жаңарту серверлерінен алу үшін қауіпсіздік бағдарламасының интерфейсіндегі жаңарту көзі ретінде Kaspersky жаңарту серверлерін көрсетіңіз. Осы параметрлер туралы қосымша ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы

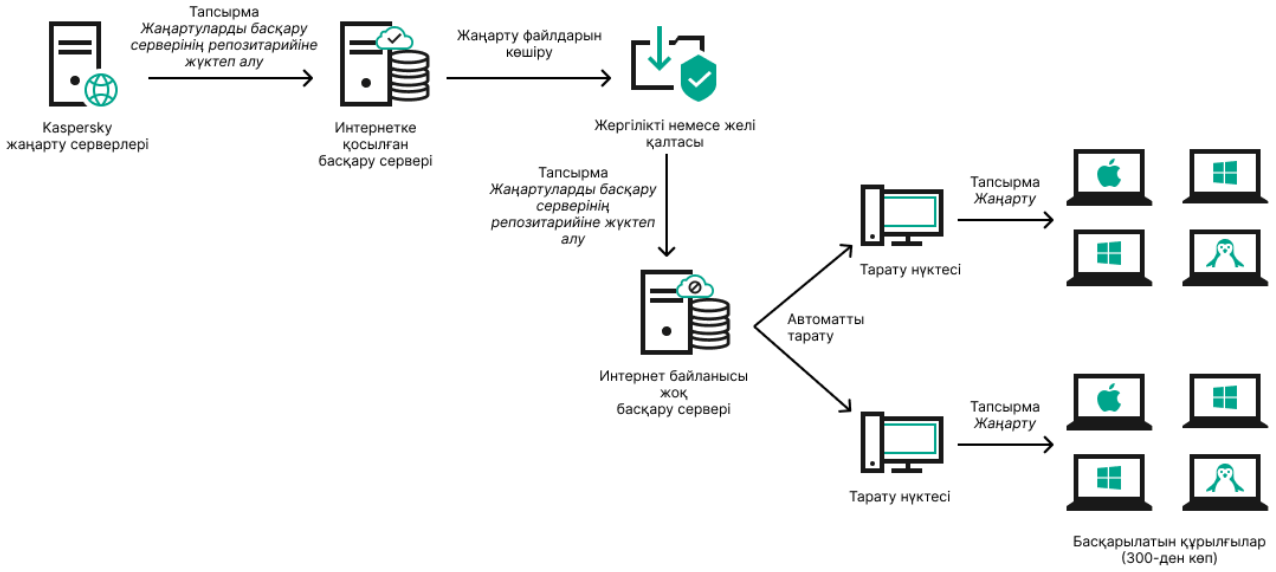
Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

Басқару серверінде интернет қосылымы болмаса, жергілікті немесе желілік қалтадан жаңартуларды жүктеу үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын конфигурациялауға болады. Бұл жағдайда, қажетті жаңарту файлдарын көрсетілген қалтаға мезгіл-мезгіл көшіріп тұру қажет. Мысалы, қажетті жаңарту файлдарын келесі көздердің бірінен көшіруге болады:

- Интернетке кіру мүмкіндігі бар Басқару сервері (төмендегі суретті қараңыз).

  Басқару сервері тек қауіпсіздік бағдарламалары сұрайтын жаңартуларды жүктейтіндіктен, Басқару серверлері басқаратын қауіпсіздік бағдарламаларының жиынтығы (интернетке қосылған және қосылмаған) сәйкес келуі керек.

Сіз жаңартуларды жүктеу үшін қолданатын Басқару серверінің нұсқасы 13.2 немесе одан да бұрынғы болса, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарын ашып, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.



Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы жаңарту

- Kaspersky Update Utility

  Утилита жаңартуларды жүктеу үшін ескі схеманы қолданатындықтан, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарын ашып, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану туралы

Kaspersky Security Center бағдарламасы Kaspersky жаңартулар серверлерінен жаңартуларды жүктеп алғанда, ол трафикті айырмашылық файлдары арқылы оңтайландырады. Сондай-ақ, желіңіздегі басқа құрылғылардан жаңартуларды қабылдайтын құрылғылардың (Басқару серверлері, тарату нүктелері және клиент құрылғылары) айырмашылық файлдарын пайдалануын қосуға болады.

Айырмашылық файлдарын жүктеу функциясы туралы

Айырмашылықтар файлы дерекқор немесе бағдарламалық модуль файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Айырмашылық файлдарын пайдалану трафикті ұйымыңыздың желісінде сақтайды, өйткені айырмашылық файлдары бүкіл дерекқор және бағдарламалық модуль файлдарына қарағанда аз орын алады. *diff файлдарды жүктеп алу* функциясы Басқару сервері немесе тарату нүктесі үшін қосылса, айырмашылық файлдары сол Басқару серверінде немесе тарату нүктесінде сақталады. Нәтижесінде, осы Басқару серверінен немесе тарату нүктелерінен жаңартулар алатын құрылғылар өздерінің дерекқорлары мен бағдарламалық модульдерін жаңарту үшін сақталған айырмашылық файлдарын пайдалана алады.

Айырмашылық файлдарын пайдалануды оңтайландыру үшін құрылғыны жаңарту кестесін Басқару серверінің жаңарту кестесімен немесе сол құрылғы жаңартуларды алатын тарату нүктелерімен синхрондау ұсынылады. Дегенмен, құрылғылар Басқару серверіне немесе құрылғы жаңартуларды алатын тарату нүктелеріне қарағанда бірнеше есе аз жаңартылса да, трафикті сақтауға болады.

Айырмашылық файлдарын жүктеу функциясын тек 11 және одан жоғары нұсқалардың Басқару серверлерінде және тарату нүктелерінде қосуға болады. Айырмашылық файлдарын Басқару серверлерінде және алдыңғы нұсқалардың тарату нүктелерінде сақтау үшін, оларды 11 немесе одан жоғары нұсқаға жаңарту қажет.

Айырмашылық файлдарын жүктеу мүмкіндігі жаңартуларды алудың офлайн моделімен үйлеспейді. Бұл дегеніміз, жаңартуларды жүктеудің офлайн моделін қолданатын Желілік агенттер айырмашылық файлдарын жүктемейді, тіпті егер бұл Желілік агенттерге жаңартулар беретін Басқару серверінде немесе тарату нүктесінде айырмашылық файлдарын жүктеу мүмкіндігі қосылса да.

Тарату нүктелері айырмашылық файлдарын автоматты түрде тарату үшін көп мекенжайлы IP таратылымын пайдаланбайды.

Айырмашылық файлдарын жүктеу функциясын қосу

Алдын ала талаптар

Сценарий үшін қажетті алғышарттар:

- Басқару сервері және тарату нүктелері 11 және одан да жоғары нұсқаға дейін жаңартылған.
- Желілік агент саясатының сипаттарында жаңартуларды алудың офлайн моделі өшірулі.

Кезеңдер

1. **Басқару серверіндегі функцияны қосу**

   Жаңартуларды Басқару серверінің қоймасына жүктеу тапсырмасының сипаттарында функцияны қосыңыз.

2. **Тарату нүктесі үшін функцияны қосу**

   Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасының көмегімен жаңартуларды алып тұратын тарату нүктесі үшін функцияны қосу

   Басқару серверінен жаңартуларды алып тұратын тарату нүктесі үшін функцияны қосыңыз.

   Бұл функция Желілік агент саясатының сипаттарында және (тарату нүктелері қолмен тағайындалған болса және саясат параметрлерін қайта анықтағыңыз келсе) Басқару серверінің сипаттарында, **Тарату нүктелері** бөлімінде қосылады.

Айырмашылық файлдарын жүктеу функциясы сәтті қосылғанын тексеру үшін сценарийді орындағанға дейін және одан кейін ішкі трафикті өлшеуге болады.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы Kaspersky Security Center-дің бағдарламаны жылдам іске қосу шебері жұмыс істеп тұрған кезде автоматты түрде жасалады. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы бір үлгіде жасалуы мүмкін. Сондықтан, сіз *Басқару сервері қоймасына жаңартуларды жүктеу* тапсырмасын ол Басқару серверінің тапсырмалар тізімінен жойылған жағдайда ғана жасай аласыз.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. Жасау процесін келесі тәсілдердің бірімен іске қосыңыз:
   - Консоль ағашының **Тапсырмалар** контекстік мәзірінде **Жаңа** → **Тапсырма** тармағын таңдаңыз.
   - **Тапсырмалар** қалтасының жұмыс аймағындағы **Тапсырма жасау** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Шебердің **Тапсырма түрін таңдау** терезесінде **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тармағын таңдаңыз.
4. **Параметрлер** шеңбері терезесінде тапсырманың келесі тапсырмаларын көрсетіңіз:
   - **Жаңартулардың көздері**

     Басқару сервері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:

     - Kaspersky жаңартулар серверлері

       Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері. Әдепкі бойынша, Басқару сервері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

       Әдепкі бойынша таңдалған.

     - Негізгі Басқару сервері

       Бұл ресурс қосалқы немесе виртуалды Басқару сервері үшін жасалған тапсырмаларға қатысты қолданылады.

     - Жергілікті немесе желілік қалта

       Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін. Желілік қалта түпнұсқалықты тексеруді қажет етсе, тек SMB протоколына қолдау көрсетіледі. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

       > Жаңарту көзі ретінде пайдаланылатын FTP серверінде, HTTP серверінде немесе желілік қалтада Kaspersky жаңарту серверлерін пайдалану кезінде жасалған қалталар құрылымына сәйкес келетін қалталар құрылымы (жаңартулармен бірге) болуы керек.

- **Басқа параметрлер**:

  - **Қосалқы Басқару серверлерін мәжбүрлеп жаңарту**

    Параметр қосылса, Басқару сервері жаңартуларды алғаннан кейін бірден бағыныңқы Басқару серверлерінде жаңартуларды алу тапсырмаларын іске қосады. Жаңарту тапсырмалары Басқару серверлеріндегі тапсырма сипаттамаларында конфигурацияланған жаңарту көзі арқылы іске қосылады.

    Егер бұл параметр өшірулі болса, қосалқы Басқару серверлеріндегі жаңарту тапсырмалары кестеге сәйкес басталады.

    Әдепкі бойынша, параметр өшірулі.

  - **Алынған жаңартуларды қосымша қалталарға көшіру**

    Егер жалауша қойылса, жаңартуларды алғаннан кейін, Басқару сервері жаңартуларды көрсетілген қалталарға көшіреді. Құрылғыңыздағы жаңартуларды қолмен басқарғыңыз келсе, осы параметрді пайдаланыңыз.

    Мысалы, сіз бұл параметрді келесі жағдайда пайдалана аласыз: ұйым желісінде бірнеше тәуелсіз ішкі желілер бар және әр ішкі желідегі құрылғылар басқа ішкі желіге қатынаса алмайды. Бұл жағдайда, барлық ішкі желілердегі құрылғылар ортақ желілік қалтаға қатынаса алады. Бұл жағдайда, ішкі желілердің біріндегі Басқару сервері үшін Kaspersky жаңарту серверлерінен жаңартуларды жүктеуді көрсетіңіз, осы параметрді қосыңыз және осы желілік қалтаны көрсетіңіз. Басқару сервері үшін жаңартуларды қоймаға жүктеу тапсырмасында дәл осы желілік қалтаны жаңартулар көзі ретінде көрсетіңіз.

    Жүктелген жаңартуларды жергілікті қалтаға көшіруді таңдасаңыз, құрылғыда Басқару сервері орнатылған қалтаны көрсетуіңіз керек. Қалтаға апаратын жол құрылғының амалдық жүйесіне байланысты. Жергілікті қалта Linux негізіндегі Басқару серверінде орналасқандықтан, POSIX жолын көрсету керек, мысалы: /path/to/dir.

    Linux негізіндегі Басқару серверінде орналасқан желілік қалтаны таңдағанда, қалтаны іске қосу арқылы Басқару сервері орнатылған құрылғыдан желілік қалтаға қатынасуды алдын ала қамтамасыз ету керек. Қалтаға қатынасу SMB протоколы арқылы жүзеге асырылады.

    Әдепкі бойынша, параметр өшірулі.

    - **Көшіру аяқталғанша құрылғыларды және қосалқы Басқару серверлерін мәжбүрлеп жаңартпау**

      Егер жалауша қойылса, клиент құрылғылары және қосалқы Басқару серверлері тарапынан жаңартуларды алу тапсырмалары, жаңартуларды желілік жаңартулар қалтасынан қосымша жаңартулар қалталарына көшіру аяқталғаннан кейін іске қосылады.

      Егер клиент құрылғылары мен қосалқы Басқару серверлері жаңартуларды қосымша желілік қалталардан жүктесе, бұл жалауша қойылуы керек.

      Әдепкі бойынша, параметр өшірулі.

  - **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу**

    14-ші нұсқадан бастап, Kaspersky Security Center бағдарламасы дерекқорлар мен бағдарлама модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Қолданба жаңартуларды жаңа схеманың көмегімен жүктеп алуы үшін, жаңарту дереккөзі жаңа схемамен үйлесімді метадеректері бар жаңарту файлдарын қамтуы керек. Жаңарту көзінде тек ескі схемамен үйлесімді метадеректері бар жаңарту файлдары болса, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз. Әйтпесе, жаңартуларды жүктеу тапсырмасы қатемен аяқталады.

Мысалы, жаңарту көзі ретінде жергілікті немесе желілік қалта көрсетілсе, ал осы қалтадағы жаңарту файлдары келесі бағдарламалардың бірімен жүктелген болса, осы параметрді қосу керек:

- Kaspersky Update Utility

  Бұл утилита жаңартуларды ескі схема бойынша жүктейді.

- Kaspersky Security Center 13.2 немесе одан бұрынғы нұсқасы

  Мысалы, бір Басқару серверінің интернетке қосылымы жоқ. Бұл жағдайда, сіз интернетке қосылған екінші Басқару сервері арқылы жаңартуларды жүктей аласыз, содан кейін жаңартуларды бірінші Сервер үшін жаңарту көзі ретінде пайдалану үшін жергілікті немесе желілік қалтаға орналастыра аласыз. Егер екінші Басқару серверінде 13.2 немесе одан төмен нұсқа нөмірі болса, бірінші Басқару серверіне арналған тапсырмада **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

Әдепкі бойынша, параметр өшірулі.

5. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

   - **Кесте бойынша іске қосу:**

     Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

     - **N сағат сайын**

       Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

     - **N күн сайын**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

     - **N апта сайын**

       Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **N минут сайын**

       Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

     - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

       Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

       Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

6. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

7. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

   Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы аяқталғаннан кейін, **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасы Басқару сервері тапсырмалары тізімінің жұмыс аймағында пайда болады.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен бағдарлама модульдерінің жаңартулары жаңартулар көзінен көшіріліп, ортақ қатынасы бар қалтада орналастырылады. Егер тапсырма басқару тобы үшін жасалса, онда ол тек көрсетілген басқару тобына кіретін Желілік агенттерге қолданылады.

Ортақ қатынасы бар қалтадан жаңартулар клиент құрылғыларына және қосалқы Басқару серверлеріне таратылады.

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау

macOS басқаруындағы тарату нүктелері Kaspersky жаңарту серверлерінен жаңартуларды жүктеп ала алмайды.

> macOS операциялық жүйесі бар құрылғылар *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының әрекет ету ауқымында болса, онда тапсырма Windows операциялық жүйесі бар құрылғылардың барлығында сәтті аяқталса да, *Сәтсіз аяқталды* мәртебесімен аяқталады.

Басқару тобы үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын жасай аласыз. Мұндай тапсырма, көрсетілген басқару тобына кіретін тарату нүктелері үшін орындалады.

Бұл тапсырманы, мысалы, Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса пайдалана аласыз. Егер тарату нүктесі прокси-сервер арқылы интернетке қосылған болса, желілік агент саясатында сәйкес параметрлерді көрсету керек.

Таңдалған басқару топтарына арналған жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. Қалтаның жұмыс аймағындағы **Жаңа тапсырма** түймесі арқылы тапсырманы жасау шеберін іске қосыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Тапсырманы жасау шеберінің **Тапсырма түрін таңдау** терезесінде **Kaspersky Security Center Басқару сервері** түйінін таңдаңыз, **Кеңейтілген** қалтасын ашыңыз және **Жаңартуларды тарату орындарының қоймаларына жүктеп алу** тапсырмасын таңдаңыз.

4. **Параметрлер** шеңбері терезесінде тапсырманың келесі тапсырмаларын көрсетіңіз:

- **Жаңартулардың көздері**

  Тарату нүктелері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:

  - Kaspersky жаңарту серверлері

    Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

    Әдепкі бойынша, осы нұсқа таңдалады.

  - Жергілікті немесе желілік қалта

    Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін. Желілік қалта түпнұсқалықты тексеруді қажет етсе, тек SMB протоколына қолдау көрсетіледі. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

    > Жаңарту көзі ретінде пайдаланылатын FTP серверінде, HTTP серверінде немесе желілік қалтада Kaspersky жаңарту серверлерін пайдалану кезінде жасалған қалталар құрылымына сәйкес келетін қалталар құрылымы (жаңартулармен бірге) болуы керек.

- **Жаңартулар сақталатын қалта**

  Сақталған жаңартуларды сақтау үшін көрсетілген қалтаға апаратын жол. Көрсетілген қалтаға апаратын жолды алмасу буферіне көшіруге болады. Топтық тапсырма үшін көрсетілген қалтаға апаратын жолды өзгерте алмайсыз.

- **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу**

  14-ші нұсқадан бастап, Kaspersky Security Center бағдарламасы дерекқорлар мен бағдарлама модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Бағдарлама жаңартуларды жаңа схеманың көмегімен жүктей алуы үшін, жаңарту көзі жаңа схемамен үйлесімді метадеректері бар жаңарту файлдарын қамтуы керек. Жаңарту көзінде тек ескі схемамен үйлесімді метадеректері бар жаңарту файлдары болса, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз. Әйтпесе, жаңартуларды жүктеу тапсырмасы қатемен аяқталады.

  Мысалы, жаңарту көзі ретінде жергілікті немесе желілік қалта көрсетілсе және осы қалтадағы жаңарту файлдары келесі бағдарламалардың бірімен жүктелген болса, осы параметрді қосу керек:

  - Kaspersky Update Utility

    Бұл утилита жаңартуларды ескі схема бойынша жүктейді.

  - Kaspersky Security Center 13.2 немесе одан бұрынғы нұсқасы

    Мысалы, тарату нүктесі жергілікті немесе желілік қалтадан жаңартуларды алу үшін конфигурацияланған. Бұл жағдайда, сіз интернетке қосылған Басқару серверін пайдалану арқылы жаңартуларды жүктей аласыз, содан кейін жаңартуларды тарату нүктесіндегі жергілікті қалтаға орналастыра аласыз. Басқару сервері нұсқасының нөмірі 13.2 немесе одан төмен болса, *Тарату нүктелерінің қоймаларына жаңартуларды жүктеу* тапсырмасында **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

5. **Басқару тобын таңдаңыз** шебері терезесінде **Шолу** түймесін басып, тапсырма қолданылатын басқару тобын таңдаңыз.

6. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

   - **Кесте бойынша іске қосу:**

     Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

     - **N сағат сайын**

       Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

     - **N күн сайын**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

     - **N апта сайын**

       Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **N минут сайын**

       Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

     - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

       Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

       Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **Апта сайын**

       Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

     - **Апта күндері бойынша**

       Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

     - **Ай сайын**

       Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

       Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

       Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

7. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

8. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

   Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы аяқталғаннан кейін жасалған **Жаңартуларды тарату орындарының қоймаларына жүктеп алу** тапсырмасы тиісті басқару тобындағы Желілік агенттің тапсырмалары тізімінде және **Тапсырмалар** қалтасында пайда болады.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен бағдарлама модульдерінің жаңартулары жаңартулар көзінен көшіріліп, ортақ қатынасы бар қалтада орналастырылады. Жүктелген жаңартуларды тек көрсетілген басқару тобына кіретін және жаңартуларды алу үшін нақты белгіленген тапсырмасы жоқ тарату нүктелері ғана пайдаланады.

Басқару серверінің сипаттары терезесіндегі **Бөлімдер** панелінің **Тарату нүктелері** опциясын таңдаңыз. **Жаңартулар көзі** бөліміндегі әрбір тарату нүктелерінің сипаттарында жаңартулар көзін (**Басқару серверінен шығарып алу** немесе **Жаңартуларды мәжбүрлеп жүктеу тапсырмасын пайдалану**) көрсетуге болады. Қолмен немесе автоматты түрде тағайындалған тарату нүктесі үшін, әдепкі бойынша **Басқару серверінен шығарып алу** нұсқасы таңдалады. Осындай тарату нүктелері *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының нәтижелерін қолданады.

Әрбір тарату нүктесінің сипаттарында осы тарату нүктесі үшін жеке конфигурацияланған желілік қалта көрсетілген. Қалта атаулары әртүрлі тарату нүктелері үшін әртүрлі болуы мүмкін. Сондықтан, тапсырма құрылғылар тобы үшін жасалса, тапсырманың сипаттарындағы жаңартулардың желілік қалтасын өзгерту ұсынылмайды.

Құрылғы үшін жергілікті тапсырма жасап жатсаңыз, *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының сипаттарындағы жаңартулар желілік қалтасын өзгерте аласыз.

Жаңартуларды Басқару серверінің сақтау орнына жүктеу тапсырмасының параметрлерін конфигурациялау

Жаңартуларды Басқару серверінің қоймасына жүктеу тапсырмасының параметрлерін конфигурациялау үшін:

1. **Тапсырмалар** консолі шежіресі қалтасының жұмыс аймағында, тапсырмалар тізімінен **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасын таңдаңыз.

2. Тапсырманың сипаттары терезесін келесі тәсілдердің бірімен ашыңыз:

   - Файлдың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   - Таңдалған тапсырмамен жұмыс істеу блогындағы **Тапсырма параметрлерін конфигурациялау** сілтемесі бойынша.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы сипаттары терезесі ашылады. Онда сіз жаңартуларды Басқару серверінің қоймасына жүктеп алу параметрлерін конфигурациялай аласыз.

Алынған жаңартуларды тексеру

Басқарылатын құрылғыларға жаңартуларды орнатудың алдында, оларды алдымен *Жаңартуды тексеру* тапсырмасының көмегімен жұмысқа жарамдылығы мен қателері тұрғысынан тексере аласыз. *Жаңартуды тексеру* тапсырмасы *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы аясында автоматты түрде орындалады. Басқару сервері жаңартуларды көзден жүктейді, оларды уақытша қоймада сақтайды және *Жаңартуды тексеру* тапсырмасын іске қосады. Бұл тапсырма сәтті орындалған жағдайда, жаңартулар уақытша қоймадан Басқару серверінің ортақ қатынасы бар қалтасына көшіріледі (<Kaspersky Security Center орнату қалтасы>\Share\Updates). Жаңартулар Басқару сервері жаңарту көзі болып табылатын клиент құрылғыларына қолданылады.

Егер *Жаңартуды тексеру* тапсырмасын орындау нәтижелері бойынша уақытша қоймада орналастырылған жаңартулар дұрыс емес деп танылса немесе *Жаңартуды тексеру* тапсырма қатемен аяқталса, жаңартуларды ортақ қатынасы бар қалтаға көшіру жүргізілмейді. Басқару серверінде алдыңғы жаңартулар жиынтығы қалады. **Қоймаға жаңартуларды жүктеу кезінде** кесте түрі бар тапсырмаларды іске қосу да орындалмайды. Жаңа жаңартулар жиынтығын тексеру сәтті аяқталса, бұл операциялар *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы келесі рет іске қосылған кезде орындалады.

Егер сынақ құрылғыларының кем дегенде біреуінде келесі шарттардың бірі орындалса, жаңартулар жиынтығы дұрыс емес болып саналады:

- жаңарту тапсырмасын орындау кезінде қате пайда болды;
- жаңартуларды қолданғаннан кейін, қауіпсіздік бағдарламасының тұрақты қорғаныс күйі өзгерді;
- талап бойынша тексеру тапсырмасын орындау барысында жұқтырған нысан табылды;
- Kaspersky бағдарламасының жұмыс қатесі туындады.

Егер сынақ құрылғыларының ешқайсысында аталған шарттардың ешбірі орындалмаса, жаңартулар жиынтығы дұрыс деп танылады және *Жаңартуды тексеру* тапсырмасы сәтті орындалды деп саналады.

Жаңартуды тексеру тапсырмасын жасауға кіріспес бұрын, алдын ала шарттарды орындаңыз:

1. Бірнеше сынақ құрылғысы бар басқару тобын құрыңыз. Жаңартуларды тексеру үшін сізге бұл топ қажет болады.

   Сынақ құрылғылары ретінде ұйымның желісінде ең көп таралған бағдарламалық конфигурациясы бар жақсы қорғалған құрылғыларды пайдалану ұсынылады. Бұл тәсілдеме, тексеру кезінде вирустарды анықтаудың сапасы мен ықтималдығын арттырады, сонымен қатар жалған іске қосылу қаупін азайтады. Сынақ құрылғыларында вирустар табылған кезде *Жаңартуды тексеру* тапсырмасы сәтсіз аяқталды деп саналады.

2. Kaspersky Endpoint Security for Windows немесе Kaspersky Security for Windows Server сияқты Kaspersky Security Center қолдау көрсететін бағдарлама үшін *Жаңарту* және *Зиянды бағдарламаны сканерлеу* тапсырмаларын жасаңыз. *Жаңарту* және *Зиянды бағдарламаны сканерлеу* тапсырмаларын жасау кезінде сынақ құрылғылары бар басқару тобын көрсетіңіз.

   Жаңартуды тексеру тапсырмасы *Жаңарту* және *Зиянды бағдарламаны сканерлеу* тапсырмаларын сынақ құрылғыларында рет-ретімен орындайды және осылайша, барлық жаңартулардың жаңартылғанын тексереді. Сондай-ақ, *Жаңартуды тексеру* тапсырмасын жасау кезінде *Жаңарту* және *Зиянды бағдарламаны сканерлеу* тапсырмалары анықталуы керек.

3. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын жасаңыз.

Kaspersky Security Center бағдарламасы клиент құрылғыларына таратпас бұрын алынған жаңартуларды тексеруі үшін:

1. Консоль ағашының **Тапсырмалар** қалтасының жұмыс аймағында, тапсырмалар тізімінен *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын таңдаңыз.
2. Тапсырманың сипаттары терезесін келесі тәсілдердің бірімен ашыңыз:
   - Файлдың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
   - Таңдалған тапсырмамен жұмыс істеу блогындағы **Тапсырма параметрлерін конфигурациялау** сілтемесі бойынша.
3. *Жаңартуды тексеру* тапсырмасы бар болса, **Шолу** түймесін басыңыз. Сынақ құрылғылары бар басқару тобында ашылған *Жаңартуды тексеру* тапсырмасы терезесінде.

4. *Жаңартуды тексеру* тапсырмасын бұған дейін жасамаған болсаңыз, **Жасау** түймесін басыңыз.

   Жаңа тапсырма жасау *Жаңартуды тексеру* шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

5. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттар терезесін жабу үшін **OK** түймесін басыңыз.

Жаңартуларды автоматты түрде тексеру қосылған. Енді сіз *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын іске қоса аласыз, сонда ол жаңартуларды тексеруден басталады.

Тексеру саясаттары мен көмекші тапсырмаларды конфигурациялау

Жаңартуларды тексеру тапсырмасын жасау кезінде Басқару сервері тексеру саясаттарын, сондай-ақ жаңарту және талап ету бойынша сканерлеу қосымша топтық тапсырмаларын қалыптастырады.

Жаңарту және талап ету бойынша сканерлеу қосымша топтық тапсырмаларын орындау үшін біраз уақыт қажет. Бұл тапсырмалар *Жаңартуларды тексеру* тапсырмасының шеңберінде орындалады. *Жаңартуларды тексеру* тапсырмасы *Жаңартуларды қоймаға жүктеу* тапсырмасының шеңберінде орындалады. *Жаңартуларды қоймаға жүктеу* тапсырмасының орындалу уақыты жаңарту және талап ету бойынша тексеру көмекші топтық тапсырмаларының орындалу уақытын қамтиды.

Тексеру саясаттары мен көмекші тапсырмалардың параметрлерін өзгертуге болады.

Тексеру саясатының немесе көмекші тапсырманың параметрлерін өзгерту үшін:

1. Консоль ағашында *Жаңартуларды тексеру* тапсырмасы құрылған топты таңдаңыз.
2. Топтың жұмыс аймағында келесі қойыншалардың бірін таңдаңыз:
   - **Саясаттар**, егер тексеру саясатының параметрлерін өзгерткіңіз келсе.
   - **Тапсырмалар**, егер көмекші тапсырманың параметрлерін өзгерткіңіз келсе.
3. Қойыншаның жұмыс аймағында параметрлерін өзгерткіңіз келетін саясатты немесе тапсырманы таңдаңыз.
4. Осы саясаттың (тапсырманың) сипаттары терезесін келесі тәсілдердің бірімен ашыңыз:
   - Саясаттың (тапсырманың) контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.
   - Саясаты (тапсырмасы) таңдалған жұмыс блогындағы **Саясатты конфигурациялау** (**Тапсырма параметрлерін конфигурациялау**) сілтемесі арқылы.

Жаңартуларды тексеру дұрыс жүргізілуі үшін тексеру саясаты мен көмекші тапсырмалардың параметрлерін өзгертуге қойылған келесі шектеулерді сақтау қажет:

- Көмекші тапсырмалардың параметрлерінде:
  - **Критикалық оқиға** және **Функционалдық ақау** маңыздылық деңгейлері бар оқиғалардың барлығын Басқару серверінде сақтау. Осы типтегі оқиғаларға сүйене отырып, Басқару сервері бағдарламалардың жұмысына талдау жасайды.
  - Жаңарту көзі ретінде Басқару серверін пайдаланыңыз.
  - Тапсырмалар кестесінің түрін көрсету: **Қолмен**.
- Тексеру саясатының параметрлерінде:
  - IChecker және iSwift тексеру технологияларын өшіру (**Негізгі қорғаныс → Файл қауіптерінен қорғаныс → Параметрлер → Қосымша → Тексеру технологиялары**).
  - Жұқтырған нысандармен жасалатын әрекеттерді таңдау: **Зарарсыздандыру; егер зарарсыздандыру мүмкін болмаса, жою** / **Зарарсыздандыру; егер зарарсыздандыру мүмкін болмаса, бұғаттау** / **Бұғаттау**. (**Негізгі қорғаныс → Файл қауіптерінен қорғаныс → Қауіп анықталған кездегі әрекет**).
- Тексеру саясаты мен көмекші тапсырмалар параметрлерінде:

  Егер бағдарламалық жасақтама модульдерінің жаңартуларын орнатқаннан кейін құрылғыны қайта іске қосу қажет болса, оны дереу орындау керек. Егер құрылғы қайта жүктелмесе, онда жаңартудың бұл түрін тексеру мүмкін болмайды. Кейбір бағдарламалар үшін қайта іске қосуды қажет ететін жаңартуларды орнатуға тыйым салынуы немесе орнату пайдаланушыдан расталғаннан кейін ғана орындалуы мүмкін. Бұл шектеулер тексеру саясаты мен көмекші тапсырмалар параметрлерінде өшірілуі керек.

Алынған жаңартуларды қарап шығу

Алынған жаңартулар тізімін қарап шығу үшін,

Қоймалар қалтасындағы консоль шежіресінен **Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар** салынған қалтасын таңдаңыз.

Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар қалтасының жұмыс аймағында, Басқару серверінде сақталған жаңартулар тізімі ұсынылған.

Құрылғыларға Kaspersky Endpoint Security жаңартуларын автоматты түрде орнату

Клиент құрылғыларында Kaspersky Endpoint Security бағдарламасының дерекқорлары мен модульдерін автоматты түрде жаңартуды конфигурациялауға болады.

Kaspersky Endpoint Security жаңартуларын құрылғыларға жүктеуді және автоматты түрде орнатуды конфигурациялау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. Келесі тәсілдердің бірімен **Жаңарту** түрі бар тапсырма жасаңыз:

   - **Тапсырмалар** консолі ағашы қалтасының контекстік мәзірінде **Жасау** → **Тапсырма** тармағын таңдаңыз.

   - **Жаңа тапсырма** қалтасының жұмыс аймағында **Тапсырмалар** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Шебердің **Тапсырма түрін таңдау** терезесінде **Kaspersky Endpoint Security** тапсырма түрін, содан соң **Жаңарту** тапсырма ішкі түрін таңдаңыз.

4. Шебердің келесі қадамдарын орындаңыз.

   Шебер жұмысының нәтижесінде, Kaspersky Endpoint Security үшін жаңарту тапсырмасы жасалады. Жасалған тапсырма **Тапсырмалар** қалтасының жұмыс аймағындағы тапсырмалар тізімінде көрсетіледі.

5. **Тапсырмалар** қалтасының жұмыс аймағында жасалған жаңарту тапсырмасын таңдаңыз.

6. Тапсырманың контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

7. Ашылған тапсырма сипаттары терезесіндегі **Бөлімдер** панелінде **Сипаттар** бөлімін таңдаңыз.

   Сипаттар бөлімінде жаңарту тапсырмасының параметрлерін жергілікті және ұялы режимдерде конфигурациялауға болады:

   - **Жергілікті режимде жаңарту параметрлері**: құрылғы мен Басқару серверін арасында байланыс орнатылған.

   - **Автономды режим үшін параметрлерді жаңартыңыз**: құрылғы мен Kaspersky Security Center арасында байланыс орнатылмаған (мысалы, құрылғы интернетке қосылмаған болса).

8. **Параметрлер** түймесі бойынша жаңартулар көзін таңдаңыз.

9. Бағдарлама дерекқорларымен бір уақытта бағдарлама модульдерінің жаңартуларын жүктеп алу және орнату үшін **Бағдарлама модульдерінің жаңартуларын жүктеу** параметрін таңдаңыз.

   Егер жалауша қойылса, Kaspersky Endpoint Security бағдарламасы пайдаланушыға бағдарлама модульдерінің қолжетімді жаңартулары туралы хабарлайды және жаңарту тапсырмасын орындау барысында бағдарлама модульдерінің жаңартуларын жаңарту пакетіне қосады. Жаңартулар модульдерін қолдануды конфигурациялаңыз:

   - **Критикалық және бекітілген жаңартуларды орнату**. Бағдарлама модульдерінің жаңартулары болған кезде, Kaspersky Endpoint Security бағдарламасы *Критикалық* күйі бар жаңартуларды автоматты түрде орнатады; бағдарлама модульдерінің қалған жаңартуларын – әкімші оларды орнатуды мақұлдағаннан кейін.

   - **Тек бекітілген жаңартуларды орнату**. Бағдарлама модульдерінің жаңартулары болған кезде Kaspersky Endpoint Security бағдарламасы оларды орнату мақұлданғаннан кейін, бағдарлама интерфейсі арқылы немесе Kaspersky Security Center көмегімен жергілікті түрде орнатады.

   Егер бағдарлама модульдерін жаңарту Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен танысуды және келісуді көздейтін болса, онда пайдаланушы Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен келіскеннен кейін, бағдарлама жаңартуды белгілейді.

10. Бағдарлама жүктелген жаңартуларды **Шолу** түймесі бойынша көрсетілген қалтаға сақтауы үшін **Жаңартуларды қалтаға көшіру** параметрін таңдаңыз.

11. **OK** түймесін басыңыз.

Жаңарту тапсырмасын орындау кезінде, бағдарлама Kaspersky жаңартулар серверлеріне сұрау салады.

Кейбір жаңартулар басқарылатын бағдарлама плагиндерінің соңғы нұсқаларын орнатуды талап етеді.

Жаңартуларды алудың офлайн-моделі

Басқарылатын құрылғылардағы Желілік агент жаңартуларды алу үшін Басқару серверіне қосылуы мүмкін. Мысалы, Желілік агент, кейде интернетке және жергілікті желіге қосылып тұрмайтын ноутбукқа орнатылуы мүмкін. Сондай-ақ, әкімші құрылғыларды желіге қосу уақытын шектеуі де мүмкін. Мұндай жағдайларда, Желілік агентті орнатылған құрылғылар Басқару серверінен кестеге сәйкес жаңартуларды ала алмайды. Желілік агент арқылы басқарылатын бағдарламаларды (мысалы, Kaspersky Endpoint Security) жаңарту конфигурацияланған болса, жаңарту үшін Басқару серверімен қосылым талап етіледі. Желілік агент пен Басқару сервері арасындағы қосылым болмаса, жаңарту мүмкін емес. Желілік агент пен Сервер арасындағы қосылым, Агент Серверге тек белгілі бір уақыт кезеңінде қосылатындай етіп конфигурациялануы мүмкін. Нашар жағдайда, конфигурацияланған қосылу кезеңдері байланыс болмаған кезеңдермен "қиылысса", онда дерекқорлар ешқашан жаңартылмайды. Сондай-ақ, көптеген басқарылатын бағдарламалар жаңартулар алу үшін бір уақытта Басқару серверіне жүгінетін жағдайлар болуы да мүмкін. Бұл жағдайда, Басқару сервері сұрауларға жауап беруді тоқтатуы мүмкін (DDoS шабуылы кезіндегідей).

Сипатталған мәселелерді болдырмау үшін, Kaspersky Security Center-де басқарылатын бағдарламалардың модульдері мен дерекқорлар жаңартуларын алудың офлайн-моделі іске асырылған. Бұл модель, басқару серверінің байланыс арналарының қолжетімсіздігінің уақытша мәселелеріне қарамастан жаңартуларды тарату механизмінің сенімділігін қамтамасыз етеді, сондай-ақ Басқару серверіне түсетін жүктемені азайтады. Бұл модель Басқару серверіне түсетін жүктемені де азайтады.

Жаңартуларды алудың офлайн-моделі қалай жұмыс істейді

Басқару сервері жаңартуларды алған кезде, ол Желілік агентті (ол орнатылған құрылғыларда) басқарылатын бағдарламалар үшін қажет етілетін жаңартулар туралы хабардар етеді. Желілік агенттер жаңартулар туралы ақпаратты алған кезде, олар Басқару серверінен қажетті файлдарды ертерек жүктеп алады. Бірінші рет қосылған кезде, Сервер осы Агенттің жаңартуларды жүктеуіне түрткі болады. Желілік агент клиент құрылғысында барлық жаңартуларды жүктегеннен кейін, жаңартулар құрылғыдағы бағдарламалар үшін қолжетімді болады.

Клиент құрылғысындағы басқарылатын бағдарлама жаңартуларды алу үшін Желілік агентке жүгінген кезде, Агент өзінде қажетті жаңартулардың бар ма екенін тексереді. Жаңартулар басқарылатын бағдарлама сұрау салған сәттен бастап 25 сағаттан ерте болмайтын мерзімнің ішінде Басқару серверінен алынған болса, онда Желілік агент Басқару серверіне қосылмайды және басқарылатын бағдарламаға жергілікті кэштегі жаңартуларды ұсынады. Желілік агент бағдарламаларға арналған жаңартуларды клиент құрылғыларында ұсынса, бірақ жаңарту үшін қосылым талап етілмесе, Басқару серверімен қосылым орындалмауы мүмкін.

Басқару серверіне түсетін жүктемені бөлу үшін, құрылғыдағы Желілік агент Серверге қосылып, жаңартуларды Сервер анықтаған уақыт аралығы ішінде кездейсоқ жүктейді. Уақыт аралығы, жаңартуларды жүктейтін Желілік агенті орнатылған құрылғылардың санына және жаңартулар өлшеміне байланысты. Басқару серверіне түсетін жүктемені азайту үшін, сіз Желілік агентті тарату нүктесі ретінде қолдана аласыз.

Жаңартуларды алудың офлайн-моделі өшірулі болса, жаңартулар қоймадағы жаңартуларды жүктеу тапсырмасының кестесіне сәйкес таралады.

Әдепкі бойынша, жаңартуларды алудың офлайн-моделі қосулы.

Жаңартуларды алудың офлайн-моделі, басқарылатын бағдарламалардың жаңартуларды алу тапсырмасының **Қоймаға жаңартуларды жүктеу кезінде** кестесі бар басқарылатын құрылғылар үшін ғана қолданылады. Басқарылатын құрылғылардың қалғаны үшін Басқару серверінен нақты уақытта жаңартулар алудың дәстүрлі жүйесі қолданылады.

Басқарылатын бағдарламаларда жаңартуларды Басқару серверінен емес, Kaspersky серверлерінен немесе желілік қалтадан алу конфигурацияланған болса және бұл арада, жаңартуларды алу тапсырмасының **Қоймаға жаңартуларды жүктеу кезінде** кестесі болса, онда жаңартуларды тиісті басқару топтарының Желілік агенті саясаттарының конфигурациялары арқылы алудың офлайн-моделін өшіру ұсынылады.

Жаңартуларды алудың офлайн-моделін қосу және өшіру

Жаңартуларды алудың офлайн-моделін өшіру ұсынылмайды. Өшіру салдарынан құрылғыларға жаңартуларды жеткізу кезінде ақау туындауы мүмкін. Кейбір жағдайларда, Kaspersky техникалық қолдау қызметінің мамандары сізге **Басқару серверінен жаңартулар мен антивирустық дерекқорларды алдын ала жүктеп алу** жалаушасын алып тастауды ұсынуы мүмкін. Олай болса, Kaspersky бағдарламалары үшін қоймаларға жаңартуларды жүктеу тапсырмасы конфигурацияланғанына көз жеткізуіңіз керек.

Басқару тобына арналған жаңартуларды алудың офлайн-моделін қосу немесе өшіру үшін:

1. Консоль ағашында, жаңартуларды алудың офлайн-моделі қосылуы қажет басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын ашыңыз.
3. **Саясаттар** қойыншасында Желілік агенттің саясатын таңдаңыз.
4. Саясаттың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Желілік агент саясатының сипаттары терезесі ашылады.
5. Саясат сипаттары терезесінде **Патчтарды және жаңартуларды басқару** бөлімін таңдаңыз.
6. Жаңартуларды алудың офлайн-моделін қосу немесе өшіру үшін **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)** жалаушасын сәйкесінше орнатыңыз немесе алып тастаңыз.

   Әдепкі бойынша, жаңартуларды алудың офлайн-моделі қосулы.

Соның нәтижесінде, жаңартуларды алудың офлайн-моделі қосулы немесе өшірулі болады.

Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнату

Әдепкі бойынша жүктелген жаңартулар мен патчтар бағдарламаның келесі құрамдастары үшін автоматты түрде орнатылады:

- Windows үшін Желілік агент
- Басқару консолі
- iOS MDM сервері

Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнату тек Windows жүйесінде жұмыс істейтін құрылғылар үшін қолжетімді. Бұл құрамдастар үшін жаңартулар мен патчтарды автоматты түрде орнатуды өшіруге болады. Бұл жағдайда, жүктелген жаңартулар мен патчтар, олардың күйін *Расталды* деп өзгерткеннен кейін ғана орнатылатын болады. *Анықталмаған* күйі бар жаңартулар мен патчтар орнатылмайды.

Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру

Kaspersky Security Center құрамдастарына арналған жаңартуларды автоматты түрде орнату құрылғыға Желілік агент орнатылған кезде әдепкі бойынша қосылады. Сіз оны Желілік агент орнатқан кезде өшіре аласыз немесе кейінірек саясаттың көмегімен өшіре аласыз.

Құрылғыға Желілік агентті жергілікті түрде орнатқан кезде Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды өшіру:

1. Желілік агентті құрылғыға жергілікті түрде орнатуды іске қосыңыз.
2. **Қосымша параметрлер** қадамында **"Анықталмаған" күйі бар Kaspersky Security Center құрамдастары үшін қолжетімді жаңартулар мен патчтерді автоматты түрде орнату** жалаушасын алып тастаңыз.
3. Содан кейін, шебердің нұсқауларын орындаңыз.

Құрылғыға Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату өшірулі Желілік агент орнатылады. Автоматты орнатуды кейінірек саясаттың көмегімен қосуға болады.

Орнату пакетін пайдалану арқылы құрылғыға Желілік агент орнатқан кезде Kaspersky Security Center құрамдастарына арналған жаңартуларды автоматты түрде орнатуды өшіру үшін:

1. Консоль ағашында **Қашықтан орнату** → **Орнату пакеттері** қалтасын таңдаңыз.
2. **Kaspersky Security Center Желілік агенті <нұсқа нөмірі>** пакетінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Орнату пакетінің сипаттарында, **Параметрлер** бөлімінде **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату** жалаушасын алып тастаңыз.

Басқару агенті, Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату мүмкіндігі өшірулі болып табылатын осы пакеттен орнатылады. Автоматты орнатуды кейінірек саясаттың көмегімен қосуға болады.

Желілік агентті құрылғыға орнатқан кезде жалауша қойылса (алынып тасталса), кейіннен Желілік агент саясатын пайдалану арқылы автоматты түрде орнатуды өшіруге (қосуға) болады.

Желілік агент саясатын қолдану арқылы Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнатуды қосу немесе өшіру үшін:

1. Консоль ағашында жаңартулар мен патчтарды автоматты түрде орнатуды қосу немесе өшіру қажетті Басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын ашыңыз.
3. **Саясаттар** қойыншасында Желілік агенттің саясатын таңдаңыз.
4. Саясаттың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Желілік агент саясатының сипаттары терезесі ашылады.
5. Саясат сипаттары терезесінде **Патчтарды және жаңартуларды басқару** бөлімін таңдаңыз.
6. Жаңартулар мен патчтарды автоматты түрде орнатуды қосу немесе өшіру үшін **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату** жалаушасын қойыңыз немесе алып тастаңыз.
7. Осы жалаушада құлыпты орнатыңыз.

Саясат таңдалған құрылғыларға қолданылады, ал Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату осы құрылғыларда қосылады (өшіріледі).

Жаңартуларды автоматты түрде тарату

Kaspersky Security Center клиент құрылғыларына және қосалқы Басқару серверлеріне жаңартуларды автоматты түрде таратуға және орнатуға мүмкіндік береді.

Жаңартуларды клиент құрылғыларына автоматты түрде тарату

Сіз таңдаған бағдарламаның жаңартулары жаңартуларды Басқару серверінің қоймасына жүктегеннен кейін бірден клиент құрылғыларына автоматты түрде таралуы үшін:

1. Клиент құрылғыларын басқаратын Басқару серверіне қосылыңыз.
2. Таңдалған клиент құрылғылары үшін осы бағдарламаның жаңартуларын келесі тәсілдердің бірімен тарату тапсырмасын жасаңыз:

   - Таңдалған басқару тобына кіретін клиент құрылғыларына жаңартуларды тарату керек болса, таңдалған топ үшін тапсырманы жасаңыз.
   - Әртүрлі басқару топтарына кіретін немесе басқару топтарына кірмейтін клиент құрылғыларына жаңартуларды тарату керек болса, құрылғыларды жинауға арналған тапсырманы жасаңыз.

Жаңа тапсырма жасау шебері іске қосылады. Келесі шарттарды орындау арқылы, оның нұсқауларын орындаңыз:

a. Шебердің **Тапсырма түрі** терезесінде, өзіңізге қажетті бағдарламаның түйінінде жаңартуларды тарату тапсырмасын таңдаңыз.

> **Тапсырма түрі** терезесінде көрсетілетін жаңартуларды тарату тапсырмасының атауы тапсырма жасалатын бағдарламаға байланысты. Kaspersky таңдалған бағдарламаларына арналған жаңарту тапсырмаларының атаулары туралы көбірек білу үшін осы бағдарламаларға арналған Нұсқаулықтарды қараңыз.

b. Шебердің **Кесте** терезесіндегі **Кесте бойынша іске қосу** өрісінде **Қоймаға жаңартуларды жүктеу кезінде** іске қосу нұсқасын таңдаңыз.

Нәтижесінде, жаңартуларды тарату тапсырмасы жаңартуларды Басқару сервері қоймасына жүктеген сайын таңдалған құрылғылар үшін іске қосылып тұрады.

Өзіңізге қажетті бағдарламаның жаңартуларын тарату тапсырмасы таңдалған құрылғылар үшін әлдеқашан жасалып қойған болса, онда жаңартуларды клиент құрылғыларына автоматты түрде тарату үшін **Кесте** бөліміндегі тапсырманың сипаттар терезесіндегі **Кесте бойынша іске қосу** өрісінде **Қоймаға жаңартуларды жүктеу кезінде** іске қосу нұсқасын таңдау керек.

Жаңартуларды қосалқы Басқару серверлеріне автоматты түрде тарату

Сіз таңдаған бағдарламаның жаңартулары жаңартуларды негізгі Басқару серверінің қоймасына жүктегеннен кейін бірден қосалқы Басқару серверлеріне автоматты түрде таралуы үшін:

1. Негізгі Басқару сервері түйініндегі консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. Жұмыс аймағындағы тапсырмалар тізімінен Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын таңдаңыз.
3. Таңдалған тапсырманың сипаттар терезесінің **Параметрлер** бөлімін келесі тәсілдердің бірімен ашыңыз:
   - Файлдың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
   - Таңдалған тапсырмамен жұмыс істеу блогындағы **Параметрлерді өзгерту** сілтемесі бойынша.
4. Тапсырманың сипаттар терезесінің **Параметрлер** бөлімінде **Басқа параметрлер** терезесін Басқа параметрлер бөлікшесіндегі **Конфигурациялау** сілтемесі арқылы ашыңыз.
5. Ашылған **Басқа параметрлер** терезесінде **Қосалқы Басқару серверлерін мәжбүрлеп жаңарту** жалаушасын қойыңыз.
6. Басқару серверінің жаңартуларын жүктеп алу тапсырмасының параметрлерінде тапсырма сипаттары терезесінің **Параметрлер** қойыншасында **Қосалқы Басқару серверлерін мәжбүрлеп жаңарту** жалаушасын қойыңыз.

Негізгі басқару сервері жаңартуларды алады, кестесіне қарамастан, жаңартуды жүктеп алу тапсырмалары қосалқы басқару серверлерінде автоматты түрде іске қосылады.

Негізгі басқару сервері антивирустық дерекқорларды қосалқы басқару серверлеріне орнатылған қолданбаларға сәйкес жаңартады. Негізгі басқару серверінде қосымша плагиндерді орнату және орнату пакеттерін жасау қажет емес.

Тарату нүктелерін автоматты түрде тағайындау

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Kaspersky Security Center бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды.

Тарату нүктелерін автоматты түрде тағайындау үшін:

1. Бағдарламаның басты терезесін ашыңыз.
2. Консоль ағашында тарату нүктелерін автоматты түрде тағайындауды қажет ететін Басқару сервері атауы бар түйінді таңдаңыз.
3. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
4. Басқару серверінің сипаттары терезесіндегі **Бөлімдер** панелінің **Тарату нүктелері** опциясын таңдаңыз.
5. Терезенің оң жағында **Тарату нүктелерін автоматты түрде тағайындау** параметрін таңдаңыз.

   Егер тарату нүктелерінің құрылғыларын автоматты түрде тағайындау қосулы болса, тарату нүктелерінің параметрлерін қолмен конфигурациялау, сондай-ақ тарату нүктелерінің тізімін өзгерту мүмкін емес.

6. **OK** түймесін басыңыз.

Нәтижесінде, Басқару сервері тарату нүктелерін автоматты түрде тағайындайды және олардың параметрлерін конфигурациялайды.

Құрылғыны қолмен тарату нүктесі етіп тағайындау

Kaspersky Security Center құрылғыларды тарату нүктелеріне тағайындауға мүмкіндік береді.

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Бұл жағдайда, Kaspersky Security Center бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды. Алайда, егер сіз қандай да бір себептермен тарату нүктелерін автоматты түрде тағайындаудан бас тартқыңыз келсе (мысалы, арнайы бөлінген серверлерді пайдаланғыңыз келсе), тарату нүктелерінің саны мен конфигурациясын алдын ала есептеу арқылы оларды қолмен тағайындауға болады.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Құрылғыны қолмен тарату нүктесі етіп тағайындау үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесінде, **Тарату нүктелері** бөлімінде **Қосу** түймесін басыңыз. **Тарату нүктелерін қолмен тағайындау** нұсқасы таңдалса, түйме қолжетімді болмайды.

   Тарату нүктесін қосу терезесі ашылады.

4. **Тарату нүктесін қосу** терезесінде келесі әрекеттерді орындаңыз:

   a. Тарату нүктесі ретінде әрекет ететін құрылғыны таңдаңыз (басқару тобында немесе құрылғының IP мекенжайын көрсетіңіз). Құрылғыны таңдау кезінде тарату нүктелерінің жұмысының ерекшеліктерін және тарату нүктесінің рөлін атқаратын құрылғыға қойылатын талаптарды ескеріңіз.

   b. Тарату нүктесі жаңартуларды тарататын құрылғылар жиынтығын көрсетіңіз. Басқару тобын немесе желілік орналасудың сипаттамасын көрсете аласыз.

5. **OK** түймесін басыңыз.

   Қосылған тарату нүктесі **Тарату нүктелері** бөліміндегі тарату нүктелерінің тізімінде пайда болады

6. Тізімнен қосылған тарату нүктесін таңдап, **Сипаттар** түймесі арқылы оның сипаттары терезесін ашыңыз.

7. Сипаттар терезесінде тарату нүктесінің параметрлерін конфигурациялаңыз:

   - **Жалпы** бөлімінде тарату нүктесінің клиент құрылғыларымен өзара әрекеттесу параметрлерін көрсетіңіз.

     - **SSL порты**

       SSL протоколын қолдана отырып, клиент құрылғыларының тарату нүктесіне қауіпсіз қосылу жүзеге асырылатын SSL портының нөмірі.

       Әдепкі бойынша порт нөмірі – 13000.

     - **Көп мекенжайлық жіберуді пайдалану**

       Егер параметр қосулы болса, орнату пакеттерін топ шегіндегі клиент құрылғыларына автоматты түрде тарату үшін көп мекенжайлы IP таратылымы қолданылады.

       Көп мекенжайлы IP таратылымы бағдарламаларды орнату пакетінен клиент құрылғылары тобына орнатуға кететін уақытты азайтады, бірақ бағдарламаны бір клиент құрылғысына орнатқан кезде орнату уақытын арттырады.

     - **IP таратудың мекенжайы**

       Көп мекенжайлы таратылым орындалатын IP мекенжайы. IP мекенжайын 224.0.0.0 – 239.255.255.255 ауқымында белгілеуге болады

       Әдепкі бойынша Kaspersky Security Center бағдарламасы белгіленген диапазонда бірегей көп мекенжайлы IP таратылымының мекенжайын тағайындайды.

     - **IP тарату портының нөмірі**

       Көп мекенжайлы таратылым портының нөмірі.

       Әдепкі бойынша порт нөмірі – 15001. Басқару сервері орнатылған құрылғы тарату нүктесі ретінде көрсетілсе, онда SSL протоколы арқылы қосылу үшін әдепкі бойынша 13001-порт қолданылады.

- **Жаңартуларды тарату**

  Жаңартулар келесі көздерден басқарылатын құрылғыларға қолданылады:

  - Бұл параметр қосулы болса, бұл тарату нүктесі болады.
  - Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе Kaspersky жаңартулар серверлері.

  Егер сіз жаңартуларды тарату үшін тарату нүктелерін қолдансаңыз, трафикті үнемдей аласыз, себебі жүктеме санын азайтасыз. Сондай-ақ, Басқару серверіндегі жүктемені азайтуға және жүктемені тарату нүктелері арасында қайта бөлуге болады. Трафик пен жүктемені оңтайландыру үшін желідегі тарату нүктелерінің санын есептеп шығаруға болады.

  Егер сіз бұл параметрді өшірсеңіз, жаңарту жүктемелері мен Басқару серверіне түсетін жүктеме артуы мүмкін. Әдепкі бойынша, параметр қосулы.

- **Орнату пакеттерін тарату**

  Орнату пакеттері келесі көздерден басқарылатын құрылғыларға қолданылады:

  - Бұл параметр қосулы болса, бұл тарату нүктесі болады.
  - Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе Kaspersky жаңартулар серверлері.

  Егер сіз орнату пакеттерін тарату үшін тарату нүктелерін қолдансаңыз, трафикті үнемдей аласыз, себебі жүктеме санын азайтасыз. Сондай-ақ, Басқару серверіндегі жүктемені азайтуға және жүктемені тарату нүктелері арасында қайта бөлуге болады. Трафик пен жүктемені оңтайландыру үшін желідегі тарату нүктелерінің санын есептеп шығаруға болады.

  Егер сіз бұл параметрді өшірсеңіз, орнату пакеттері жүктемелері мен Басқару серверіне түсетін жүктеме артуы мүмкін. Әдепкі бойынша, параметр қосулы.

- **Тарату нүктесін хабарландыратын сервер ретінде қолдану**

  Kaspersky Security Center бағдарламасында тарату нүктесі ұялы протокол бойынша басқарылатын құрылғылар үшін push сервері ретінде жұмыс істеуі мүмкін. Мысалы, егер сіз KasperskyOS орнатылған құрылғыларды Басқару серверімен мәжбүрлеп синхрондауды қосқыңыз келсе, push сервері қосулы болуы керек. Push серверінде, push сервері қосылған тарату нүктесімен бірдей басқарылатын құрылғылар аймағы бар. Егер сізде бір басқару тобына тағайындалған бірнеше тарату нүктелері болса, олардың әрқайсысында ескерту серверін қосуға болады. Бұл жағдайда, Басқару сервері жүктемені тарату нүктелері арасында бөледі.

  KasperskyOS операциялық жүйесі орнатылған құрылғыларды басқарсаңыз немесе мұны жасауды жоспарласаңыз, тарату нүктесін push сервері ретінде пайдалануыңыз керек. Клиент құрылғыларына push хабарландыруларын жібергіңіз келсе, тарату нүктесін push сервері ретінде пайдалануға болады.

- **Push серверінің порты**

  Клиент құрылғылары қосылу үшін қолданатын тарату нүктесінің порты. Әдепкі бойынша порт нөмірі – 13295.

- **Әрекет ету ауқымы** бөлімінде тарату нүктесі жаңартуларды тарататын аймақты көрсетіңіз (басқару топтары және/немесе желілік орындар).

- **KSN Проксиі** бөлімінде қолданбаны тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын жіберу үшін пайдаланылатындай етіп конфигурациялауға болады.

  - **Тарату нүктелері тарапынан KSN Проксиін қосу**

    KSN прокси-сервері қызметі тарату нүктесі ретінде әрекет ететін құрылғыда орындалады. Бұл параметрді желі трафигін қайта тарату және оңтайландыру үшін пайдаланыңыз.

    Тарату нүктесі Kaspersky Security Network мәлімдемесінде көрсетілген KSN статистикасын Kaspersky ұйымына жібереді.

    Әдепкі бойынша, параметр өшірулі. Осы параметрді қосу, **Басқару серверін прокси-сервер ретінде пайдалану** және **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрлері Басқару серверінің сипаттары терезесінде қосылған жағдайда ғана күшіне енеді.

    Суық резерві бар істен шығуға төзімді кластер түйініне (белсенді / пассивті) тарату нүктесін тағайындауға және сол түйінде KSN прокси-серверін қосуға болады.

  - **Басқару серверіне KSN сұрауын жіберу**

    Тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын Басқару серверіне жібереді.

    Әдепкі бойынша, параметр қосулы.

  - **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру**

    Тарату нүктесі KSN-ге басқарылатын құрылғылардан KSN немесе KPSN бұлттық қызметіне сұраулар жібереді. Тарату нүктесінде жасалған KSN сұраулары да тікелей KSN Cloud немесе KPSN-ге жіберіледі.

    Желілік агенттің 11 (немесе одан бұрынғы) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алмайды. Тарату нүктелерін KSN сұрауларын KSN-ге жіберу үшін қайта реттегіңіз келсе, әрбір тарату нүктесі үшін **KSN сұрауын Басқару серверіне қайта жіберу** параметрін қосыңыз.

    Желілік агенттің 12 (және одан да жоғары) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алады.

  - **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу**

    Егер прокси-сервер параметрлері тарату нүктелерінің немесе Желілік агенттің сипаттарында конфигурацияланған болса, бірақ сіздің желіңіздің архитектурасы KPSN бағдарламасын тікелей пайдалануды талап етсе, осы жалаушаны қойыңыз. Әйтпесе, басқарылатын қолданбадан сұрау KPSN қолданбасына берілмейді.

    Бұл параметр **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру** параметрін таңдаған жағдайда қолжетімді болады.

  - **TCP порты**

    Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын TCP портының нөмірі. Әдепкі бойынша 13111-порт орнатылған.

  - **UDP порты**

    Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

- **HTTPS порты**

  Басқарылатын құрылғылардың KSN прокси-серверіне HTTPS порты арқылы қосылуын қаласаңыз, **HTTPS пайдалану** параметрін қосыңыз және **HTTPS порты арқылы** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, KSN прокси-серверіне қосылу 17111 HTTPS порты арқылы жүзеге асырылады.

- **Құрылғыны табу** бөлімінде Windows домендерінің, Active Directory және IP ауқымдарының сауалнамасын тарату нүктесі арқылы конфигурациялаңыз.

  - **Windows домендері**

    Сіз Windows домендеріне арналған құрылғыларды анықтауды қосып, оның кестесін белгілей аласыз.

  - **Active Directory**

    Сіз Active Directory сауалнамасын қосып, сауалнама кестесін белгілей аласыз.

    Windows операциялық жүйесі бар тарату нүктесін пайдалансаңыз, келесі нұсқалардың бірін таңдауға болады:

    - **Ағымдағы Active Directory доменінде сауалнама өткізу**.
    - **Active Directory домендер тобында сауалнама өткізу**.
    - **Таңдалған Active Directory домендерінде сауалнама өткізу**. Егер сіз осы нұсқаны таңдасаңыз, тізімге бір немесе бірнеше Active Directory доменін қосыңыз.

    Желілік агенттің 15-нұсқасы орнатылған Linux операциялық жүйесімен жұмыс істейтін тарату нүктесін пайдалансаңыз, мекенжай мен пайдаланушының есептік жазба деректерін көрсеткен Active Directory домендеріне ғана сауалнама жүргізуге болады. Ағымдағы Active Directory домені мен Active Directory доменінің тобы үшін сауалнама жүргізу қолжетімді емес.

  - **IP ауқымдары**

    IPv4 ауқымдары мен IPv6 желілері үшін құрылғыларды табу функциясын қосуға болады.

    Ауқым сауалнамасын қосу параметрін қоссаңыз, сауалнама ауқымын қосып, сауалнама кестесін белгілеуге болады. IP ауқымдарын сауалнама ауқымдары тізіміне қоса аласыз.

    IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану параметрін қоссаңыз, тарату нүктесі нөлдік конфигурациясы бар желіні қолдана отырып, IPv6 желісіне сауалнама өткізеді (бұдан әрі *Zeroconf* деп те аталады). Бұл жағдайда, көрсетілген IP ауқымдары еленбейді, өйткені тарату нүктесі бүкіл желіге сауалнама өткізеді. **IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану** параметрі, тарату нүктесі Linux басқаруымен жұмыс істеп тұрса қолжетімді. Zeroconf IPv6 сауалнамасын пайдалану үшін тарату нүктесінде avahi-browse утилитасын орнату қажет.

- **Кеңейтілген** бөлімінде тарату нүктесі таратылатын деректерді сақтау үшін пайдалануы керек қалтаны көрсетіңіз.

  - **Әдепкі қалтаны пайдалану**

    Деректерді сақтау үшін осы нұсқаны таңдағанда, тарату нүктесінде Желілік агент орнатылған қалта қолданылады.

  - **Көрсетілген қалтаны пайдалану**

    Бұл нұсқаны таңдағанда, төмендегі өрісте қалта жолын көрсетуге болады. Қалта тарату нүктесінде де, қашықтан да, ұйым желісінің құрамына кіретін кез келген құрылғыда орналастырылуы мүмкін.

    Тарату нүктесінде Желілік агент іске қосылатын есептік жазба оқу және жазу үшін көрсетілген қалтаға қатынасу мүмкіндігіне ие болуы керек.

Нәтижесінде, таңдалған құрылғылар тарату нүктелерінің рөлін атқарады.

Тек Windows операциялық жүйесі жұмыс істейтін құрылғылар өздерінің желілік орындарын анықтай алады. Желілік орынды анықтау басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін қолжетімді емес.

Құрылғыны тарату нүктелері тізімінен алып тастау

Құрылғыны тарату нүктелері тізімінен алып тастау үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару серверінің сипаттары терезесінде, **Тарату нүктелері** бөлімінде тарату нүктесінің функцияларын орындайтын құрылғыны таңдап, **Жою** түймесін басыңыз.

Соның нәтижесінде, құрылғы тарату нүктелері тізімінен алынып, тарату нүктесінің функцияларын орындауды доғарады.

Құрылғыны Басқару сервері автоматты түрде тағайындаған болса, оны тарату нүктелері тізімінен жоюға болмайды.

Тарату нүктелері арқылы жаңартуларды жүктеп алу

Kaspersky Security Center бағдарламасы, тарату нүктелеріне Басқару серверінен, Kaspersky серверлерінен, жергілікті немесе желілік қалтадан жаңартулар алып тұруға мүмкіндік береді.

Жаңарту дереккөзін көрсету қажет болмаса, *Жаңартуларды тарату нүктелерінің қоймаларына жүктеп алу* тапсырмасын пайдалануға кеңес береміз. Мәліметтер алу үшін келесі тақырыпты қараңыз: Жаңартуларды тарату нүктелерінің қоймаларына жүктеп алу тапсырмасын жасау.

Тарату нүктесі үшін жаңартулар алуды конфигурациялау үшін келесі әрекеттерді орындаңыз:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесіндегі **Тарату нүктелері** бөлімінде топтың клиент құрылғыларына жаңартулар жеткізілетін тарату нүктесін таңдаңыз.
4. **Сипаттар** түймесі арқылы, таңдалған тарату нүктесі сипаттары терезесін ашыңыз.
5. Тарату нүктесі сипаттары терезесінде **Жаңартулардың көздері** бөлімін таңдаңыз.

6. Тарату нүктесі үшін жаңартулар көзін таңдаңыз:

   - Тарату нүктесі Басқару серверінен жаңартуларды алып тұруы үшін, **Басқару серверінен шығарып алу** нұсқасын таңдаңыз:

     - **Айырмашылық файлдарын жүктеп алу**

       Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

       Әдепкі бойынша, параметр қосулы.

   - Тарату нүктесі тапсырманың көмегімен жаңартулар алып тұруы үшін, **Жаңартуларды мәжбүрлеп жүктеу тапсырмасын пайдалану** нұсқасын таңдаңыз:

     - Мұндай тапсырма құрылғыда әлдеқашан бар болса, **Таңдау** түймесін басыңыз және пайда болған тізімнен тапсырманы таңдаңыз.

     - Мұндай тапсырма құрылғыда әлі болмаса, тапсырманы жасау үшін **Жаңа тапсырма** түймесін басыңыз. Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасы жергілікті болып табылады. Тарату нүктесі ретінде әрекет ететін әрбір құрылғы үшін тапсырманы бөлек жасау керек.

Нәтижесінде, тарату нүктесі көрсетілген көзден жаңартулар алып тұрады.

Қоймадан бағдарламалық жасақтама жаңартуларын жою

Бағдарламалық жасақтама жаңартуларын Басқару сервері қоймасынан жою үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама жаңартулары** салынған қалтасын таңдаңыз.

2. **Бағдарламалық жасақтама жаңартулары** қалтасының жұмыс аймағында жою қажет жаңартуды таңдаңыз.

3. Жаңартудың контекстік мәзірінде **Жаңартулар файлдарын жою** тармағын таңдаңыз.

Бағдарламалық жасақтама жаңартулары Басқару серверінің қоймасынан жойылады.

Кластерлік модельде Kaspersky бағдарламасына арналған патч орнату

Kaspersky Security Center, кластерлік модельде Kaspersky бағдарламаларына арналған патчтарды қолмен орнатуды ғана қолдайды.

Кластерлік модельде Kaspersky бағдарламасына арналған патч орнату үшін:

1. Кластердің әр түйініне патч жүктеңіз.
2. Белсенді түйінде патч орнатуды іске қосыңыз.
3. Патчтың сәтті орнатылуын күтіңіз.
4. Кластердің барлық қосалқы түйіндерінде патчты дәйекті түрде іске қосыңыз.

   Патчты пәрмен жолынан іске қосу кезінде "`-CLUSTER_SECONDARY_NODE`" кілтін қолданыңыз.

   Осы әрекеттер нәтижесінде патч кластердің әр түйінінде орнатылады.
5. Kaspersky кластерлік қызметтерін қолмен іске қосыңыз.

Кластердің әр түйіні Басқару консольде Желілік агенті орнатылған құрылғы ретінде көрсетіледі.

Орнатылған патчтер туралы ақпаратты **Бағдарламалық жасақтама жаңартулары** қалтасында немесе Kaspersky бағдарламалық жасақтама модулі жаңартуларының нұсқалары туралы есепте көруге болады.

Клиент құрылғыларындағы үшінші тарап бағдарламалары бағдарламаларын басқару

Kaspersky Security Center бағдарламасы клиент құрылғыларында орнатылған Kaspersky және басқа өндірушілердің бағдарламаларын басқаруға мүмкіндік береді.

Әкімші келесі әрекеттерді орындай алады:

- Берілген критерийлер негізінде бағдарламалар санаттарын құру.
- Арнайы жасалған ережелерді қолдана отырып, бағдарламалардың санаттарын басқару.
- Құрылғыларда бағдарламалардың іске қосылуын басқару.
- Құрылғыларда орнатылған бағдарламалық жасақтаманы түгендеу және тізімдемесін жүргізу.
- Құрылғыларда орнатылған бағдарламалық жасақтаманың осалдығын түзету.
- Құрылғыларда Windows Update және басқа бағдарламалық жасақтама өндірушілерінің жаңартуларын орнату.
- Лицензиялық бағдарламалар топтары үшін лицензиялық кілттердің қолданылуын қадағалау.

Үшінші тарап бағдарламалары туралы

Kaspersky Security Center клиент құрылғыларында орнатылған үшінші тарап бағдарламалық жасақтамасын жаңартуға және үшінші тарап бағдарламалық жасақтамасының осалдықтарын түзетуге көмектеседі. Kaspersky Security Center үшінші тарап бағдарламаларын тек ағымдағы нұсқадан соңғы нұсқаға дейін жаңарта алады.

Үшінші тарап бағдарламалық жасақтамаларының тізімін өзгертуге болады және ол динамикалық түрде жаңартылады. MMC негізіндегі басқару консолі мен Kaspersky Security Center Web Console-дегі қолжетімді жаңартулар тізімін қарап шығып, үшінші тарап бағдарламалық жасақтамасын (пайдаланушылардың құрылғыларында орнатылған) Kaspersky Security Center көмегімен жаңарта алатыныңызды тексере аласыз.

Төменде сипатталған процедура Kaspersky Security Center арқылы жаңартуға болатын үшінші тарап бағдарламалық жасақтамаларының тізімін көруге ғана арналған. Ешбір тапсырманы бастамастан тиісті ақпаратқа арнайы мүмкіндіктер арқылы қол жеткізу үшін қадамдар орындалады.

Kaspersky Security Center көмегімен жаңартуға болатын үшінші тарап бағдарламалық жасақтамаларының тізімін Kaspersky Security Center Web Console-ден көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Шебердің **Жаңа тапсырма параметрлері** қадамында келесі параметрлерді көрсетіңіз:

   a. **Бағдарлама** ашылмалы тізімінде **Kaspersky Security Center** опциясын таңдаңыз.

   b. **Тапсырма түрі** тізімінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырма түрін таңдаңыз.
4. Шебердің **Тапсырма ауқымы** қадамында **Басқарылатын құрылғылар** опциясын таңдаңыз.
5. Шебердің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** қадамында **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
6. Шебердің **Ереже түрін таңдаңыз** қадамында **Үшінші тарап жаңартуларға арналған ереже** опциясын таңдаңыз.
7. Шебердің **Жалпы шарттар** қадамында **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)** опциясын таңдап, **Келесі** түймесін басыңыз.

Үшінші тарап бағдарламалық жасақтамасының тізімі көрсетіледі.

MMC негізіндегі консольде Kaspersky Security Center арқылы жаңартуға болатын үшінші тарап бағдарламалық жасақтамаларының тізімін көру үшін сізге Осалдықтар мен патчтарды басқару лицензиясы қажет. Әйтпесе **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасы қолжетімді болмайды.

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
2. Жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.
3. **Тапсырма жасау** түймесі арқылы жаңа тапсырма жасау шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.
4. Шебердің **Тапсырма түрін таңдау** бетіндегі **Қажетті жаңартуларды орнату және осалдықтарды түзету** опциясын таңдаңыз.
5. Шебердің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** қадамында **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
6. Шебердің **Ереже түрін таңдаңыз** қадамында **Үшінші тарап жаңартуларға арналған ереже** опциясын таңдаңыз.
7. Шебердің **Жалпы шарттар** қадамында **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)** опциясын таңдап, **Келесі** түймесін басыңыз.

Үшінші тарап бағдарламалық жасақтамасының тізімі көрсетіледі.

Үшінші тарап бағдарламаларының жаңартуларын орнату

Kaspersky Security Center бағдарламасы клиент құрылғыларына орнатылған бағдарламалық жасақтаманың жаңартуларын басқаруға, сондай-ақ қажетті жаңартуларды орнату арқылы Microsoft бағдарламалары мен басқа да бағдарламалық жасақтама өндірушілері бағдарламаларында осалдықтарды түзетуге мүмкіндік береді.

Kaspersky Security Center жаңартуларды іздеу тапсырмасы арқылы жаңартуларды іздейді және жаңартуларды жаңарту қоймасына жүктейді. Жаңартуларды іздеу аяқталғаннан кейін, бағдарлама әкімшіге қолжетімді жаңартулар және осы жаңартулармен түзетілетін бағдарламалардағы осалдықтар туралы ақпарат береді.

Қолжетімді Microsoft Windows жаңартулары туралы ақпарат Windows Update орталығынан беріледі. Басқару серверін Windows Update (WSUS) сервері ретінде пайдалануға болады. Басқару серверін Windows Update сервері ретінде пайдалану үшін жаңартуларды Windows Update-пен синхрондауды конфигурациялау қажет. Деректерді Windows Update орталығымен синхрондауды конфигурациялағаннан кейін, Басқару сервері құрылғылардағы Windows Update қызметтеріне жаңартуларды белгіленген жиілікпен орталықтан ұсынады.

Бағдарламалық жасақтама жаңартуларын Желілік агенттің саясаты арқылы да басқаруға болады. Ол үшін Желілік агент саясатын құрып, тиісті саясатты құру шеберінің терезелерінде бағдарламалық жасақтаманы жаңарту параметрлерін конфигурациялау қажет.

Әкімші **Бағдарламаларды басқару** қалтасының құрамына кіретін **Бағдарламалық жасақтама жаңартулары** қалтасында қолжетімді жаңартулар тізімін қарай алады. Бұл қалтада Microsoft корпорациясының және құрылғыларға таратылуы мүмкін басқа бағдарламалық жасақтама өндірушілерінің Басқару сервері алған жаңартулардың тізімі бар. Қолжетімді жаңартулар туралы ақпаратты көргеннен кейін, әкімші жаңартуларды құрылғыларға орната алады.

Kaspersky Security Center кейбір бағдарламаларын жаңарту, бағдарламаның алдыңғы нұсқасын жою және жаңа нұсқасын орнату арқылы орындалады.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Негізгі және қосымша басқару серверлері үшін **Интерфейсті конфигурациялау** терезесінде **Осалдықтар мен патчтарды басқаруды көрсету** опциясы қосылғанына көз жеткізіңіз. Әйтпесе, жаңарту іздеу тапсырмасы тек WSUS жаңартуларын өңдейді.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап бағдарламалық жасақтамасы жаңартулары Kaspersky технологиялары арқылы зиянды БҚ-дың бар-жоғы тұрғысынан автоматты түрде тексеріледі. Бұл технологиялар файлдарды автоматты түрде тексеру үшін қолданылады және антивирустық тексеруді, статикалық талдауды, динамикалық талдауды, "құмсалғыштың" жүріс-тұрысын талдауды және машиналық оқытуды қамтиды.

Kaspersky мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап бағдарламалық жасақтамасы жаңартуларын қолмен талдамайды. Сонымен қатар Kaspersky мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

Жаңартуларды барлық құрылғыларға орнатпас бұрын, орнатылған жаңартулар құрылғылардағы бағдарламалардың дұрыс жұмыс істемеуіне көз жеткізу мақсатында тексеру үшін орнатуды орындауға болады.

Сценарий: Үшінші тарап бағдарламаларын жаңарту

Бұл бөлімде клиент құрылғыларында орнатылған үшінші тарап бағдарламаларын жаңарту сценарийі ұсынылған. Үшінші тарап бағдарламалары Microsoft және басқа да бағдарламалық жасақтама өндірушілері ұсынған бағдарламаларды қамтиды. Microsoft бағдарламалары үшін жаңартуларды Windows Update қызметі ұсынады.

Алдын ала талаптар

Microsoft бағдарламаларынан басқа үшінші тарап бағдарламаларының жаңартуларын орнату үшін Басқару серверінде интернет байланысы болуы керек.

Әдепкі бойынша, Басқару сервері Microsoft бағдарламасының жаңартуларын басқарылатын құрылғыларға орнату үшін интернет байланысын қажет етпейді. Мысалы, басқарылатын құрылғылар Microsoft бағдарламасының жаңартуларын тікелей Microsoft жаңарту серверлерінен немесе ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server серверінен жүктей алады. Басқару серверін WSUS сервері ретінде қолдансаңыз, Басқару сервері интернетке қосылуы керек.

Кезеңдер

Өндірушілердің жаңартуы келесі кезеңдерден тұрады:

1. **Қажетті жаңартуларды іздеу**

   Басқарылатын құрылғыларға қажет үшінші тарап бағдарламасының жаңартуларын табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосыңыз. Бұл тапсырма аяқталғаннан кейін, Kaspersky Security Center бағдарламасы құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап бағдарламалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады.

   Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы Басқару серверінің Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Егер сіз шеберді іске қоспаған болсаңыз, тапсырма жасаңыз немесе бағдарламаны жылдам іске қосу шеберін іске қосыңыз.

   Нұсқаулар:

   - Басқару консолі: Бағдарламаларда осалдықтарды іздеу, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін кестені белгілеу.
   - Kaspersky Security Center Web Console: Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы параметрлері.

2. **Табылған жаңартулар тізімін талдау**

   Бағдарламалық жасақтама жаңартулары тізімін қарап, қандай жаңартуларды орнату керектігін шешіңіз. Әрбір жаңарту туралы толық ақпаратты көру үшін тізімдегі жаңарту атын түртіңіз. Тізімдегі әрбір жаңарту үшін клиент құрылғыларындағы жаңартуларды орнату статистикасын да көруге болады.

   Нұсқаулар:

   - Басқару консолі: Қолжетімді жаңартулар туралы ақпаратты қарау.
   - Kaspersky Security Center Web Console: Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау.

3. **Жаңартулар орнатуды конфигурациялау**

   Kaspersky Security Center бағдарламасы үшінші тарап бағдарламаларының жаңартулар тізімін алғаннан кейін, сіз оларды *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын немесе *Windows Update жаңартуларын орнату* тапсырмасын қолдану арқылы клиент құрылғыларына орната аласыз. Осы тапсырмалардың бірін жасаңыз. Осы тапсырмаларды **Тапсырмалар** қойындысында немесе **Бағдарламалық жасақтама жаңартулары** тізімі көмегімен жасай аласыз.

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы Windows Update жаңартулары қызметі ұсынатын жаңартуларды және басқа өндірушілердің бағдарламаларын қоса алғанда, Microsoft бағдарламаларына арналған жаңартуларды орнату үшін қолданылады. Назар аударыңыз, Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана осы тапсырманы жасауға болады.

   Windows Update жаңартуларын орнату тапсырмасы лицензияны қажет етпейді, бірақ оны Windows Update жаңартуларын орнату үшін ғана қолдануға болады.

Бағдарламалық жасақтаманың кейбір жаңартуларын орнату үшін сіз бағдарламалық жасақтаманы орнатуға арналған Лицензиялық келісімді қабылдауыңыз керек. Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтама жаңартулары орнатылмайды.

Жаңартуды орнату тапсырмасын кесте бойынша іске қосуға болады. Тапсырманың кестесін көрсету кезінде, жаңартуды орнату тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама осалдықтарын түзету, Қолжетімді жаңартулар туралы ақпаратты қарау.
- Kaspersky Security Center Web Console: Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау, Windows Update жаңартуларын орнату тапсырмасын жасау, Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау.

4 Тапсырманың кестесін белгілеу

Жаңартулар тізімі әрқашан өзекті екеніне көз жеткізу мақсатында, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын мезгіл-мезгіл автоматты түрде іске қосылуы үшін, оны іске қосу кестесін белгілеңіз. Әдепкі бойынша *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы сағат 18:00:00-де қолмен іске қосылады.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, сіз оны *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосумен бірдей немесе одан сирек жиілікпен іске қосуды белгілей аласыз. *Windows Update жаңартуларын орнату* тапсырмасын жоспарлау кезінде, бұл тапсырма үшін, осы тапсырманы іске қосудың алдында әрбір рет жаңартулар тізімін анықтауыңыз керек екеніне назар аударыңыз.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5 Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау (қажет болса)

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, сіз тапсырманың сипаттарында жаңартуларды орнату ережелерін көрсете аласыз. Windows Update жаңартуларын орнату тапсырмасын жасаған болсаңыз, бұл қадамды өткізіп жіберіңіз.

Әрбір ереже үшін, жаңарту күйіне байланысты орнату үшін жаңартуларды анықтай аласыз: *Анықталмаған*, *Расталды* немесе *Қабылданбады*. Мысалы, сіз серверлер үшін белгілі бір тапсырма жасай аласыз және тек Windows Update жаңартуларын ғана және тек *Расталды* күйі бар жаңартуларды ғана орнатуға рұқсат беру үшін осы тапсырмаға арналған ережені орната аласыз. Содан кейін, орнатқыңыз келетін жаңартулар үшін *Расталды* күйін қолмен белгілейсіз. Бұл жағдайда, *Анықталмаған* немесе *Қабылданбады* күйі бар Windows Update жаңартулары тапсырмада көрсетілген серверлерге орнатылмайды.

Жаңартуларды орнатуды басқарған кезде, аздаған жаңартулар үшін *Расталды* күйін қолданған жөн. Бірнеше жаңарту орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасында конфигурациялауға болатын ережелерді қолданыңыз. *Расталды* күйін, ережелерде көрсетілген өлшемшарттарға сай келмейтін жаңартулар үшін ғана белгілеу ұсынылады. Жаңартулардың көп санын қолмен растау кезінде, Басқару серверінің өнімділігі төмендеп, бұл Басқару серверінің артық жүктелуіне әкелуі мүмкін.

Әдепкі бойынша, жүктелген бағдарламалық жасақтама жаңартулары *Анықталмаған* күйіне ие. Күйді **Бағдарламалық жасақтама жаңартулары** (**Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары**) тізімінде *Расталды* немесе *Қабылданбады* деп өзгерте аласыз.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
- Kaspersky Security Center Web Console: Үшінші тарап бағдарламалары жаңартуларын растау және қабылдамау

6. **Басқару серверін Windows Server Жаңарту қызметтері (WSUS) ретінде жұмыс істеу үшін конфигурациялау (қажет болса)**

   Әдепкі бойынша, Windows Update жаңартулары Microsoft серверлерінен басқарылатын құрылғыларға жүктеледі. Басқару серверін WSUS сервері ретінде пайдалану үшін осы параметрді өзгерте аласыз. Бұл жағдайда, Басқару сервері жаңарту деректерін белгіленген жиілікпен Windows Update қызметімен синхрондайды және жаңартуларды желілік құрылғылардағы Windows Update қызметтеріне орталықтандырылған түрде ұсынады.

   Басқару серверін WSUS сервері ретінде қолдану үшін, сіз Windows Update жаңартуларын синхрондау тапсырмасын жасап, Желілік агент саясатында **Басқару серверін WSUS сервері ретінде пайдалану** жалаушасын қойыңыз.

   Нұсқаулар:

   - Басқару консолі: Windows Update жаңартуларын Басқару серверімен синхрондау, Желілік агент саясатында Windows жаңартуларын конфигурациялау
   - Kaspersky Security Center Web Console: Windows Update жаңартуларын синхрондау тапсырмасын жасау

7. **Жаңартуларды орнату тапсырмасын іске қосу**

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын немесе *Windows Update жаңартуларын орнату* тапсырмасын іске қосыңыз. Осы тапсырмаларды орындағаннан кейін, жаңартулар жүктеледі және басқарылатын құрылғыларға орнатылады. Тапсырма аяқталғаннан кейін, оның тапсырмалар тізімінде *Сәтті аяқталды* күйі бар екеніне көз жеткізіңіз.

8. **Үшінші тарап бағдарламаларының жаңартуларын орнату нәтижелері туралы есепті құрастыру (қажет болса)**

   Жаңартуды орнату статистикасын қарау үшін, **Үшінші тарап бағдарламалық жасақтамасы жаңартуларын орнату нәтижелерін хабарлау** құрастырыңыз.

   Нұсқаулар:

   - Басқару консолі: Есепті жасау және қарау
   - Kaspersky Security Center Web Console: Есепті жасау және қарау

Нәтижелер

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған және конфигурациялаған болсаңыз, жаңартулар басқарылатын құрылғыларға автоматты түрде орындалатын болады. Жаңа жаңартуларды Басқару сервері қоймасына жүктеу кезінде, Kaspersky Security Center бағдарламасы жаңартулардың жаңарту ережелерінде көрсетілген критерийлерге сәйкес келетіндігін тексереді. Критерийлерге сәйкес келетін барлық жаңа жаңартулар келесі тапсырма басталған кезде автоматты түрде орнатылады.

Windows Update жаңартуларын орнату тапсырмасын жасаған болсаңыз, *Windows Update жаңартуларын орнату* тапсырмасының сипаттарында көрсетілетін жаңартулар ғана орнатылады. Кейінірек, Басқару сервері қоймасына жүктелген жаңа жаңартуларды орнатқыңыз келсе, қолданыстағы тапсырманың жаңарту тізіміне қажетті жаңартуларды қосу немесе *Windows Update жаңартуларын орнату* тапсырмасын жасау қажет болады.

Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау

Клиент құрылғыларында орнатылған үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін көру үшін,

Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама жаңартулары** салынған қалтасын таңдаңыз.

Қалтаның жұмыс аймағында сіз құрылғыларда орнатылған бағдарламалар үшін қолжетімді жаңартулар тізімін көре аласыз.

Жаңарту сипаттарын көру үшін,

Бағдарламалық жасақтама жаңартулары қалтасының жұмыс аймағында, жаңартудың контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

Жаңарту сипаттары терезесінде келесі ақпарат қарау үшін қолжетімді:

- **Жалпы** бөлімінде **Жаңартуды растау күйі** қарай аласыз:
  - **Анықталмаған** – жаңарту жаңартулар тізімінде қолжетімді, бірақ орнатуға мақұлданбаған.
  - **Расталды** – жаңарту жаңартулар тізімінде қолжетімді және орнатуға мақұлданған.
  - **Қабылданбады** – жаңарту орнату үшін қабылданбады.
- **Атрибуттар** бөлімінде **Автоматты түрде орнатылады** өрісінің мәндерін көре аласыз:
  - *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы бағдарлама үшін жаңартуларды орната алса, **Автоматты түрде** мәні көрсетіледі. Тапсырма үшінші тарап бағдарламаларын өндіруші ұсынған веб-мекенжайдан жаңа жаңартуларды автоматты түрде орнатады.
  - Егер Kaspersky Security Center бағдарламасы бағдарламаға арналған жаңартуларды автоматты түрде орната алмаса, **Қолмен** мәні көрсетіледі. Сіз жаңартуларды қолмен орната аласыз.

  Автоматты түрде орнатылады өрісі Windows бағдарламаларының жаңартулары үшін көрсетілмейді.
- Жаңарту қолданылатын клиент құрылғыларының тізімі.
- Жаңарту алдында (кез келген) орнатылуы тиіс жүйелік құрамдастардың (алдын ала талаптардың) тізімі.
- Бұл жаңартуды түзететін бағдарламалардағы осалдықтар.

Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау

Жаңартуларды орнату тапсырмасының параметрлері, орнатылуы тиісті жаңартуларды мақұлдауды талап етуі мүмкін. Орнату қажет болған жаңартуларды растай аласыз немесе орнатылмауы тиісті жаңартулардан бас тарта аласыз.

Мысалы, сіз алдымен жаңартуларды сынақ ортасында орнатуды тексеріп, олар құрылғылардың жұмысына кедергі келтірмейтіндігіне көз жеткізіп алып, содан кейін осы жаңартуларды клиент құрылғыларына орната аласыз.

Үшінші тарап бағдарламаларының жаңартуларын орнатуды басқару үшін *Расталды* күйін қолдану, жаңартулардың аз саны үшін орынды болып саналады. Үшінші тарап бағдарламаларының бірнеше жаңартуларын орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасында конфигурациялауға болатын ережелерді қолданыңыз. *Расталды* күйін, ережелерде көрсетілген өлшемшарттарға сай келмейтін жаңартулар үшін ғана белгілеу ұсынылады. Жаңартулардың көп санын қолмен растау кезінде, Басқару серверінің өнімділігі төмендеп, бұл Басқару серверінің артық жүктелуіне әкелуі мүмкін.

Бір немесе бірнеше жаңартуды растау немесе болдырмау үшін:

1. Консоль ағашында **Кеңейтілген → Бағдарламаларды басқару → Бағдарламалық жасақтама жаңартулары** түйінін таңдаңыз.

2. **Бағдарламалық жасақтама жаңартулары** қалтасының жұмыс аймағында жоғарғы оң жақтағы **Жаңарту** сілтемесі арқылы өтіп, жаңартулар тізімінің жүктелгенін күтіңіз. Жаңартулардың тізімі көрсетіледі.

3. Растау немесе қабылдамау қажет болған жаңартуларды таңдаңыз.

   Таңдалған нысанмен жұмыс істеу блогы жұмыс аймағының оң жағында көрсетіледі.

4. Таңдалған жаңартуларды растау үшін **Жаңартуды растау күйі** ашылмалы тізімінен **Расталды** тармағын таңдаңыз немесе таңдалған жаңартуларды қабылдамау үшін **Қабылданбады** тармағын таңдаңыз.

   Әдепкі бойынша, **Анықталмаған** мәні көрсетілген.

Расталды күйі белгіленген жаңартулар орнату кезегіне қойылады.

Қабылданбады күйі белгіленген жаңартулар, бұған дейін орнатылған құрылғылардан жойылады (бұл мүмкін болса). Сондай-ақ, олар құрылғыларға кейінірек орнатылмайды.

Kaspersky бағдарламаларына арналған жаңартулардың кейбірін жою мүмкін емес. Оларға **Қабылданбады** күйін белгілеген болсаңыз, Kaspersky Security Center бағдарламасы осы жаңартуларды бұған дейін орнатылған құрылғылардан жоймайды. Мұндай жаңартулар болашақта құрылғыларға ешқашан орнатылмайды. Kaspersky қолданбаларына арналған жаңартуды жою мүмкін болмаса, бұл сипат жаңарту сипаттары терезесінде көрсетіледі: **Бөлімдер** панеліндегі **Жалпы** опциясын таңдаңыз, сонда жұмыс аймағындағы сипат **Орнату кезіндегі талаптар** бөлімінде пайда болады. Үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін **Қабылданбады** күйін белгілеп жатсаңыз, бұл жаңартулар орнатылуы жоспарланған, бірақ әлі орнатылмаған құрылғыларға орнатылмайды. Жаңартулар әлдеқашан орнатылған құрылғыларда қала береді. Оларды жою қажет болса, мұны жергілікті түрде қолмен орындай аласыз.

Windows Update жаңартуларын Басқару серверімен синхрондау

Жылдам іске қосу шеберінің **Жаңартуларды басқару параметрлері** терезесінде **Басқару серверін WSUS сервері ретінде пайдалану** опциясын таңдасаңыз, Windows жаңартуды синхрондау тапсырмасы автоматты түрде жасалады. Тапсырманы **Тапсырмалар** қалтасында іске қосуға болады. Microsoft бағдарламалық жасақтамасын жаңарту функциясы **Windows Update жаңартуларын синхрондау** тапсырмасы сәтті аяқталғаннан кейін ғана қолжетімді.

Microsoft бағдарламалық жасақтамасының жаңартулары 10 ГБ-тан асуы мүмкін. Басқару серверінің дерекқоры осындай томдарды өзіне сыйғыза алатынына көз жеткізіңіз, әйтпесе **Windows Update жаңартуларын синхрондау** тапсырмасы орындалмайды. Microsoft SQL Express дерекқорына **Windows Update жаңартуларын синхрондау** тапсырмасы үшін қолдау көрсетілмейді.

Windows Update жаңартуларын синхрондау тапсырмасы Microsoft серверлерінен тек метадеректерді ғана жүктейді. Егер желіде WSUS сервері пайдаланылмаса, онда әрбір клиент құрылғысы Microsoft жаңартуларын сыртқы серверлерден дербес жүктейді.

Windows Update жаңартуларын Басқару серверімен синхрондау тапсырмасын жасау үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама жаңартулары** салынған қалтасын таңдаңыз.

2. **Қосымша әрекеттер** түймесін басыңыз да, ашылатын тізімнен **Windows Update жаңартуларын синхрондауды конфигурациялау** мәнін таңдаңыз.

   Шеберде **Windows Update жаңартуларын синхрондау** тапсырмасы жасалып, **Тапсырмалар** қалтасында көрсетіледі.

   Windows Update жаңарту орталығынан деректерді алу тапсырмасын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Windows Update жаңартуларын синхрондау тапсырмасын **Тапсырмалар** қалтасында **Тапсырма жасау** түймесі арқылы жасауға да болады.

Microsoft өз серверлерінен ескірген жаңартуларды мезгіл-мезгіл жойып отырады, осылайша өзекті жаңартулар саны 200 000-нан 300 000-ға дейін құрайды. Пайдаланылатын диск кеңістігін және дерекқор өлшемін азайту үшін Kaspersky Security Center бағдарламасы Microsoft жаңарту серверлерінде жоқ ескірген жаңартуларды жояды.

Windows Update жаңартуларын синхрондау тапсырмасын орындау барысында, бағдарлама Microsoft жаңартулар серверінен өзекті жаңартулар тізімін алады. Содан соң, Kaspersky Security Center бағдарламасы ескірген жаңартулар тізімін анықтайды. **Осалдықтарды және қажетті жаңартуларды іздеу** тапсырмасын келесі жолы іске қосқан кезде, Kaspersky Security Center бағдарламасы ескірген жаңартуларды белгілеп, жою уақытын белгілейді. **Windows Update жаңартуларын синхрондау** тапсырмасын келесіде іске қосқан кезде, 30 күн бұрын жою жалаушасы қойылған барлық жаңарту жойылады. Kaspersky Security Center 180 күннен артық уақыт бұрын жою жалаушасы қойылған ескі жаңартуларды да тексеріп, оларды жояды.

Windows Update жаңартуларын синхрондау тапсырмасының жұмысы аяқталғаннан және дерекқорларда ескірген жаңартулар жойылғаннан кейін, жойылған жаңартулар файлдарының хеш-кодтары, сондай-ақ олар бұған дейін жүктелген болса, %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles қалтасында оларға сай келетін файлдар қалып қоюы мүмкін. Басқару серверіне техникалық қызмет көрсету тапсырмасының көмегімен мұндай ескірген жазбаларды дерекқордан және оларға сай келетін файлдардан жоюға болады.

1-қадам. Трафикті азайту қажеттілігін анықтау

Kaspersky Security Center бағдарламасы жаңартуларды Microsoft Windows Update Servers серверлерімен синхрондағанда, барлық файлдар туралы ақпарат Басқару серверінің дерекқорында сақталады. Сондай-ақ, дискіге Windows жаңарту агентімен өзара әрекеттесу кезінде жаңартуға қажетті барлық файлдар жүктеледі. Атап айтқанда, Kaspersky Security Center жедел орнату файлдары туралы ақпаратты дерекқорға сақтайды және қажет болған жағдайда жүктейді. Жедел орнату файлдарын жүктеу дискідегі бос орынды қысқартуға себеп болады.

Диск кеңістігінің қысқаруын азайту және трафикті төмендету үшін **Жедел орнату файлдарын жүктеу** параметрін өшіруге болады.

Егер параметр таңдалса, тапсырманы орындау барысында жедел орнату файлдары жүктеледі. Әдепкі бойынша нұсқа таңдалмаған.

2-қадам. Бағдарламалар

Бұл бөлімде жаңартулар жүктелетін бағдарламаларды таңдауға болады.

Барлық бағдарламалар жалаушасы қойылған болса, онда жаңартулар барлық қолданыстағы бағдарламалар үшін, сондай-ақ болашақта шығарылуы мүмкін бағдарламалар үшін жүктеледі.

Әдепкі бойынша, **Барлық бағдарламалар** жалаушасы қойылған.

3-қадам. Жаңартулар санаттары

Бұл бөлімде Басқару серверіне жүктелетін жаңарту санаттарын таңдауға болады.

Барлық санаттар жалаушасы қойылған болса, онда жаңартулар барлық қолданыстағы жаңарту санаттары үшін, сондай-ақ болашақта пайда болуы мүмкін санаттар үшін жүктеледі.

Әдепкі бойынша, **Барлық санаттар** жалаушасы қойылған.

4-қадам. Жаңартулардың локализация тілі

Бұл терезеде Басқару серверіне жүктелетін жаңартулардың локализация тілдерін таңдауға болады. Жаңартулардың локализация тілдерін жүктеудің келесі нұсқаларының бірін таңдаңыз:

- **Барлық тілдерді, соның ішінде жаңаларын жүктеп алу**

  Егер бұл нұсқа таңдалса, жаңартулардың барлық қолжетімді локализация тілдері Басқару серверіне жүктеледі. Әдепкі бойынша, осы нұсқа таңдалған.

- **Таңдалған тілдерді жүктеп алу**

  Егер бұл нұсқа таңдалса, тізімде Басқару серверіне жүктелетін жаңартулардың локализация тілдерін таңдауға болады.

5-қадам. Тапсырманы іске қосу үшін есептік жазбаны таңдау

Тапсырманы іске қосу үшін есептік жазбаны таңдау терезесінде тапсырманы қандай есептік жазбамен іске қосу керектігін көрсетуге болады. Келесі нұсқалардың бірін таңдаңыз:

- **Әдепкі есептік жазба**

  Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Есептік жазбаны көрсету**

  Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

  - **Есептік жазба**

    Тапсырманы іске қосатын есептік жазба.

  - **Құпиясөз**

    Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

6-қадам. Тапсырма кестесін конфигурациялау

Тапсырма кестесін конфигурациялау терезесінде тапсырманы бастау кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

- **Кесте бойынша іске қосу:**

  Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

  - **N сағат сайын**

    Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

  - **N күн сайын**

    Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

  - **N апта сайын**

    Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

    Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

  Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

  Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Бір рет**

  Тапсырма көрсетілген күн мен уақытта тек бір рет орындалады (тапсырманың жасалған күніне сәйкес).

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

7-қадам. Тапсырманың атауын анықтау

Тапсырма атауын анықтау терезесінде жасалатын ереженің атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды (`"*<>?\:|`) қамтуы мүмкін емес. Әдепкі мән — *Windows Update жаңартуларын синхрондау*.

8-қадам. Тапсырманы жасауды аяқтау

Тапсырманы жасауды аяқтау терезесінде шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Жасалған Windows Update жаңартуларын синхрондау тапсырмасы консоль шежіресінің **Тапсырмалар** қалтасындағы тапсырмалар тізімінде көрсетіледі.

Құрылғыларға жаңартуларды қолмен орнату

Жылдам іске қосу шеберінің **Жаңартуларды басқару параметрлері** бетінде **Қажетті жаңартуларды іздеу және орнату** опциясын таңдасаңыз, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы автоматты түрде жасалады. Тапсырмасы **Басқарылатын құрылғылар** қалтасының **Тапсырмалар** қойыншасында тоқтатуға немесе іске қосуға болады.

Бағдарламаны жылдам іске қосу шеберінде **Қажетті жаңартуларды іздеу** нұсқасын таңдасаңыз, бағдарламалық жасақтама жаңартуларын клиент құрылғыларына *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасының көмегімен орната аласыз.

Сіз келесі әрекеттердің бірін орындай аласыз:

- Жаңартуларды орнату үшін тапсырма жасаңыз.
- Қолданыстағы жаңартуларды орнату тапсырмасына жаңартуды орнату ережесін қосыңыз.
- Қолданыстағы жаңартуларды орнату тапсырмасының параметрлерінде жаңартуларды сынап орнатуды конфигурациялаңыз.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Жаңартуларды орнату тапсырмасын жасау арқылы жаңартуларды орнату

Сіз келесі әрекеттердің бірін орындай аласыз:

- Қажетті жаңартуларды орнату үшін тапсырма жасаңыз.
- Жаңартуды таңдап, оны орнату және ұқсас жаңартуларды орнату үшін тапсырма жасаңыз.

Қажетті жаңартуларды орнату үшін:

1. Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама жаңартулары** салынған қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында орнатқыңыз келетін жаңартуды таңдаңыз.
3. Келесі әрекеттердің бірін орындаңыз:
   - Таңдалған жаңартудың контекстік мәзірінде **Жаңартуды орнату → Жаңа тапсырма** тармағын таңдаңыз.
   - Таңдалған файлдармен жұмыс блогында **Жаңартуды орнату (тапсырма жасау)** сілтемесі бойынша.
4. Бағдарламаның барлық алдыңғы нұсқаларын орнату терезесі ашылады. Таңдалған жаңартуларды орнату үшін қажет болса, бағдарлама нұсқаларын дәйекті түрде орнатуға келіссеңіз, **Иә** түймесін басыңыз. Егер сіз нұсқаларды дәйекті түрде орнатпай, бағдарламаны тікелей жаңартқыңыз келсе, **Жоқ** түймесін басыңыз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

   Жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау шебері ашылады. Содан кейін, шебердің нұсқауларын орындаңыз.

5. **Операциялық жүйені қайта іске қосу опциясын таңдау** шебері терезесінде операциядан кейін клиент құрылғыларындағы операциялық жүйені қайта қосу қажет болса, орындалатын әрекетті таңдаңыз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

   - **Құрылғыны қайта іске қосу**

     Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

   - **Пайдаланушыдан әрекетті орындауды сұрау**

     Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

     - **Сұрауды қайталау жиілігі (мин)**

       Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

       Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

     - **Келесі уақыттан кейін қайта іске қосу (мин)**

       Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

   - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

     Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

     Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

     Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

     Әдепкі бойынша, параметр өшірулі.

6. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

   - **Кесте бойынша іске қосу:**

     Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

     - **N сағат сайын**

       Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

     - **N күн сайын**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

     - **N апта сайын**

       Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **N минут сайын**

       Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

     - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

       Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

       Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **Апта сайын**

       Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

     - **Апта күндері бойынша**

       Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

     - **Ай сайын**

       Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

       Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

       Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

7. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

8. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

   Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы нәтижесінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасы жасалып, **Тапсырмалар** қалтасында көрсетіледі.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасының сипаттарында жаңартуды орнатудың алдында жалпыжүйелік құрамдастарды (алғышарттарды) автоматты түрде орнатуды қоса аласыз. Параметр қосулы болған кезде барлық қажетті жүйелік құрамдастар жаңартудан бұрын орнатылады. Бұл құрамдастардың тізімін жаңарту сипаттарынан көруге болады.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасының сипаттарында бағдарламаны жаңа нұсқасына дейін жаңартатын жаңартуларды орнатуға рұқсат бере аласыз.

Егер тапсырма параметрлері үшінші тарап жаңартуларын орнату ережелерін орнатса, Басқару сервері өндірушілердің сайтынан қажетті жаңартуларды жүктейді. Жаңартулар Басқару серверінің қоймасында сақталады және олар қолданылатын құрылғыларға таратылып, орнатылады.

Егер тапсырма параметрлерінде Microsoft жаңартуларын орнату ережелері конфигурацияланса және Басқару сервері WSUS сервері ретінде пайдаланылса, онда Басқару сервері қажетті жаңартуларды қоймаға жүктеп, басқарылатын құрылғыларға таратады. Егер желіде WSUS сервері пайдаланылмаса, онда әрбір клиент құрылғысы Microsoft жаңартуларын сыртқы серверлерден дербес жүктейді.

Қажетті жаңартуды және ұқсас жаңартуларды орнату үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама жаңартулары** салынған қалтасын таңдаңыз.

2. жұмыс аймағында орнатқыңыз келетін жаңартуды таңдаңыз.

3. **Жаңартуларды орнату шеберін іске қосу** түймесін басыңыз.

   Жаңартуды орнату шеберін іске қосылады.

   > Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері функционалы қолжетімді болады.

   Содан кейін, шебердің нұсқауларын орындаңыз.

4. **Жаңартуды орнатудың бар тапсырмаларын іздеу** бетінде келесі параметрлерді көрсетіңіз:

   - **Осы жаңартуды орнататын тапсырмаларды іздеу**

     Егер бұл параметр қосулы болса, жаңартуды орнату шебері таңдалған жаңартуды орнату үшін бұрыннан бар тапсырманы іздейді.

     Егер бұл параметр өшірулі болса немесе тиісті тапсырма табылмаса, жаңартуды орнату шебері жаңартуды орнату үшін ереже немесе тапсырма жасауды ұсынады.

     Әдепкі бойынша, параметр қосулы.

   - **Жаңартуды орнатуды бекіту**

     Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

     Әдепкі бойынша, параметр өшірулі.

5. Егер сіз жаңартуларды орнату үшін бұрыннан бар тапсырманы іздеуді таңдасаңыз және бірнеше сәйкес тапсырмалар табылса, сол тапсырмалардың сипаттарын қарап шығуға немесе оларды қолмен іске қосуға болады. Қосымша әрекеттер қажет емес.

   Әйтпесе, **Жаңа жаңартуды орнату тапсырмасы** түймесін басыңыз.

6. Оны жаңа тапсырмаға қосу үшін орнату ережесінің түрін таңдап, **Дайын** түймесін басыңыз.

7. Бағдарламаның барлық алдыңғы нұсқаларын орнату терезесі ашылады. Таңдалған жаңартуларды орнату үшін қажет болса, бағдарлама нұсқаларын дәйекті түрде орнатуға келіссеңіз, **Иә** түймесін басыңыз. Егер сіз нұсқаларды дәйекті түрде орнатпай, бағдарламаны тікелей жаңартқыңыз келсе, **Жоқ** түймесін басыңыз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

   Жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау шебері ашылады. Содан кейін, шебердің нұсқауларын орындаңыз.

8. **Операциялық жүйені қайта іске қосу опциясын таңдау** шебері терезесінде операциядан кейін клиент құрылғыларындағы операциялық жүйені қайта қосу қажет болса, орындалатын әрекетті таңдаңыз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

   - **Құрылғыны қайта іске қосу**

     Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

   - **Пайдаланушыдан әрекетті орындауды сұрау**

     Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

     - **Сұрауды қайталау жиілігі (мин)**

       Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

       Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

     - **Келесі уақыттан кейін қайта іске қосу (мин)**

       Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

   - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

     Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

Әдепкі бойынша, параметр өшірулі.

9. Шебердің **Тапсырма белгіленетін құрылғыларды таңдау** бетінде келесі нұсқалардың бірін таңдаңыз:

- **Басқару серверімен анықталған желілік құрылғыларды таңдау**

  Бұл жағдайда, тапсырма арнайы құрылғыларға тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

  Мысалы, сіз бұл параметрді Желілік агентті тағайындалмаған құрылғыларға орнату тапсырмасында пайдалана аласыз.

- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

  Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

  Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**

  Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

  Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

- **Басқару тобына тапсырманы белгілеу**

  Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

  Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

  Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

10. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

- **Кесте бойынша іске қосу:**

  Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

  - **N сағат сайын**

    Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

- **N күн сайын**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N апта сайын**

  Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

  Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

  Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен** (әдепкі бойынша таңдалған)

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

> Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

11. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

12. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

    Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы аяқталғаннан кейін, **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасы жасалып, **Тапсырмалар** қалтасында көрсетіледі.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Бағдарламаның жаңа нұсқасын орнатқаннан кейін, құрылғыларда орнатылған және жаңартылатын бағдарламаның жұмысына байланысты басқа бағдарламалардың жұмысы бұзылуы мүмкін.

Қолданыстағы тапсырмаға ереже қосу арқылы жаңартуды орнату

Қолданыстағы тапсырмаға ереже қосу арқылы жаңартуды орнату үшін:

1. Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама жаңартулары** салынған қалтасын таңдаңыз.

2. жұмыс аймағында орнатқыңыз келетін жаңартуды таңдаңыз.

3. **Жаңартуларды орнату шеберін іске қосу** түймесін басыңыз.

   Жаңартуды орнату шеберін іске қосылады.

   > Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері функционалы қолжетімді болады.

   Содан кейін, шебердің нұсқауларын орындаңыз.

4. **Жаңартуды орнатудың бар тапсырмаларын іздеу** бетінде келесі параметрлерді көрсетіңіз:

   - **Осы жаңартуды орнататын тапсырмаларды іздеу**

     Егер бұл параметр қосулы болса, жаңартуды орнату шебері таңдалған жаңартуды орнату үшін бұрыннан бар тапсырманы іздейді.

     Егер бұл параметр өшірулі болса немесе тиісті тапсырма табылмаса, жаңартуды орнату шебері жаңартуды орнату үшін ереже немесе тапсырма жасауды ұсынады.

     Әдепкі бойынша, параметр қосулы.

   - **Жаңартуды орнатуды бекіту**

     Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

     Әдепкі бойынша, параметр өшірулі.

5. Егер сіз жаңартуларды орнату үшін бұрыннан бар тапсырманы іздеуді таңдасаңыз және бірнеше сәйкес тапсырмалар табылса, сол тапсырмалардың сипаттарын қарап шығуға немесе оларды қолмен іске қосуға болады. Қосымша әрекеттер қажет емес.

   Әйтпесе, **Жаңартуды орнату ережесін қосу** түймесін басыңыз.

6. Ереже қосқыңыз келетін тапсырманы таңдап, **Ереже қосу** түймесін басыңыз.

   Сондай-ақ, бұрыннан бар тапсырмалардың сипаттарын көруге, оларды қолмен іске қосуға немесе тапсырма жасауға болады.

7. Таңдалған тапсырмаға қосылатын ереже түрін таңдап, **Дайын** түймесін басыңыз.

8. Бағдарламаның барлық алдыңғы нұсқаларын орнату терезесі ашылады. Таңдалған жаңартуларды орнату үшін қажет болса, бағдарлама нұсқаларын дәйекті түрде орнатуға келіссеңіз, **Иә** түймесін басыңыз. Егер сіз нұсқаларды дәйекті түрде орнатпай, бағдарламаны тікелей жаңартқыңыз келсе, **Жоқ** түймесін басыңыз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

Жаңартуды орнатуға арналған жаңа ереже бұрыннан бар **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасына қосылған.

Жаңартуларды тексеріп орнатуды конфигурациялау

Жаңартуларды тексеріп орнатуды конфигурациялау үшін:

1. Консоль тармағында **Тапсырмалар** қойындысындағы **Басқарылатын құрылғылар** қалтасының **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасын таңдаңыз.

2. Тапсырманың контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы сипаттары терезесі ашылады.

3. **Тексеру үшін орнату** бөліміндегі тапсырма сипаттары терезесінде тексеріп орнатудың қолжетімді нұсқаларының бірін таңдаңыз:

   - **Сканерлемеу**. Жаңартуларды тексеріп орнатқыңыз келмесе, осы нұсқаны таңдаңыз.

   - **Таңдалған құрылғыларда сканерлеуді іске қосу**. Белгілі бір құрылғыларда жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Қосу** түймесін басып, жаңартуларды тексеріп орнату қажет құрылғыларды таңдаңыз.

   - **Көрсетілген топтағы құрылғыларда сканерлеуді іске қосу**. Құрылғылар тобында жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Сынақ топты белгілеңіз** өрісінде тексеріп орнату қажет құрылғылар тобын көрсетіңіз.

   - **Құрылғылардың көрсетілген пайызында сканерлеуді іске қосу**. Құрылғылардың бөліктеріне жаңартуларды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Құрылғылардың жалпы санынан сынақ құрылғылардың пайызы** өрісінде жаңартуларды тексеріп орнату қажет құрылғылар пайызын көрсетіңіз.

4. **Сканерлемеу** параметрінен басқа кез келген параметрді таңдалғаннан кейін, **Орнатуды жалғастыру туралы шешімді қабылдау уақытының мөлшері, сағ** өрісінде жаңартуларды сынап орнатқаннан бастап жаңартуларды барлық құрылғыларға орната бастағанға дейін қанша сағат өтуі керектігін көрсетіңіз.

Желілік агент саясатында Windows жаңартуларын конфигурациялау

Желілік агент саясатында Windows жаңартуларын конфигурациялау үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** тармағын таңдаңыз.

2. Жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.

3. Желілік агент саясатын таңдаңыз.

4. Саясаттың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Желілік агент саясатының сипаттары терезесі ашылады.

5. **Бөлімдер** тақтасында **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** тармағын таңдаңыз.

6. Windows жаңартуларын Басқару серверіне жүктеу, содан кейін оларды Желілік агент арқылы клиент құрылғыларына тарату үшін **Басқару серверін WSUS сервері ретінде пайдалану** параметрін таңдаңыз.

   Егер бұл параметр таңдалмаса, Windows жаңартулары Басқару серверіне жүктеледі. Бұл жағдайда, клиент құрылғылары Windows жаңартуларын тікелей Microsoft серверлерінен алады.

7. Пайдаланушылар Windows Update көмегімен өз құрылғыларында орната алатын жаңартулар жиынтығын таңдаңыз.

   > Windows 10 операциялық жүйелері бар құрылғылар үшін, Windows Update-те құрылғыларға арналған жаңартулар табылса, онда сіз **Пайдаланушыларға Windows Update жаңартуларын орнатуды басқаруға рұқсат беру** астында таңдаған жаңа параметр, табылған жаңартуларды орнатқаннан кейін ғана қолданылады.

   Ашылмалы тізімнен параметрді таңдаңыз:

   - **Пайдаланушыларға барлық қолданылатын Windows Update жаңартуларын орнатуға рұқсат беру**

     Пайдаланушылар өз құрылғыларына қолданылатын барлық Windows Update жаңартуларын орната алады.

     Жаңартуларды орнатуға әсер еткіңіз келмесе, осы нұсқаны таңдаңыз.

     > Пайдаланушы Windows Update жаңартуларын қолмен орнатқан кезде, жаңартуларды Басқару серверінен емес, Microsoft серверлерінен жүктеуге болады. Бұл, Басқару сервері бұл жаңартуларды әлі жүктемеген болса жүзеге асырылуы мүмкін. Microsoft серверлерінен жаңартуларды жүктеу трафиктің өсуіне әкеледі.

   - **Пайдаланушыларға тек расталған Windows Update жаңартуларын орнатуға рұқсат беру**

     Пайдаланушылар өз құрылғыларына қолданылатын және әкімші мақұлдаған барлық Windows Update жаңартуларын орната алады.

     Мысалы, сіз алдымен жаңартуларды сынақ ортасында орнатуды тексеріп, олар құрылғылардың жұмысына кедергі келтірмейтіндігіне көз жеткізіп алып, содан кейін осы мақұлданған жаңартуларды клиент құрылғыларына орнатуға рұқсат бере аласыз.

     > Пайдаланушы Windows Update жаңартуларын қолмен орнатқан кезде, жаңартуларды Басқару серверінен емес, Microsoft серверлерінен жүктеуге болады. Бұл, Басқару сервері бұл жаңартуларды әлі жүктемеген болса жүзеге асырылуы мүмкін. Microsoft серверлерінен жаңартуларды жүктеу трафиктің өсуіне әкеледі.

   - **Пайдаланушыларға Windows Update жаңартуларын орнатуға рұқсат бермеу**

     Пайдаланушылар Windows Update жаңартуларын өз құрылғыларына қолмен орната алмайды. Барлық қолданылатын жаңартулар әкімші белгілеген конфигурацияға сәйкес орнатылады.

     Жаңартуларды орнатуды орталықтан басқарғыңыз келсе, осы нұсқаны таңдаңыз.

     Мысалы, желіні жүктемеу үшін жаңарту кестесін конфигурациялауға болады. Пайдаланушылардың өнімділігіне кедергі келтірмеу үшін жаңартуларды жұмыс уақытынан тыс жоспарлауға болады.

8. Windows Update жаңартулар іздеу режимін таңдаңыз:

   - **Белсенді**

     Егер бұл нұсқа таңдалса, Басқару сервері Желілік агенттің көмегімен клиент құрылғысындағы Windows жаңарту агентінің жаңарту көзіне: Windows Update Servers немесе WSUS серверіне жүгінуін бастайды. Содан соң, Желілік агент Windows Update агентінен алынған ақпаратты Басқару серверіне жібереді.

     Бұл параметр, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы болса ғана қолданылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Пассив**

     Егер бұл нұсқа таңдалса, Желілік агент Windows жаңарту агентін жаңарту көзімен соңғы рет синхрондау кезінде алынған жаңартулар туралы ақпаратты мезгіл-мезгіл Басқару серверіне жібереді. Windows жаңарту агентін жаңарту көзімен синхрондау орындалмаса, Басқару серверіндегі жаңартулар туралы деректер ескіреді.

     Жаңарту көзі кэшінен жаңартуларды алғыңыз келсе, осы параметрді таңдаңыз.

   - **Өшірулі**

     Егер бұл нұсқа таңдалса, Басқару сервері жаңартулар туралы ақпаратты сұрамайды.

     Мысалы, алдымен жергілікті құрылғыдағы жаңартуларды тексергіңіз келсе, осы параметрді таңдаңыз.

9. Егер іске қосу кезінде орындалатын файлдарды осалдықтардың болуы тұрғысынан тексеру қажет болса, **Іске қосу кезінде орындалатын файлдарда осалдықтар бар-жоғын сканерлеу** параметрін таңдаңыз.

10. Сіз өзгерткен барлық параметрлер үшін өңдеу бұғатталғанына көз жеткізіңіз. Әйтпесе, өзгерістер қолданылмайды.

11. **Қолдану** түймесін басыңыз.

Үшінші тарап бағдарламаларында осалдықтарды түзету

Бұл бөлімде, басқарылатын құрылғыларда орнатылған бағдарламаларда осалдықтарды түзетумен байланысты Kaspersky Security Center мүмкіндіктері сипатталған.

Сценарий: Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету

Бұл бөлімде, Windows басқаруымен жұмыс істейтін құрылғылардағы осалдықтарды анықтау және түзету сценарийі келтірілген. Операциялық жүйелердегі, үшінші тарап бағдарламаларындағы, соның ішінде Microsoft бағдарламаларындағы осалдықтарды анықтауға және түзетуге болады.

Алдын ала талаптар

- Kaspersky Security Center бағдарламасы сіздің ұйымыңызда орналастырылған.
- Ұйымыңыздың желісінде Windows басқаруымен жұмыс істейтін басқарылатын құрылғылар бар.
- Басқару серверін интернетке қосу келесі тапсырмаларды орындау үшін қажет:
  - Microsoft бағдарламалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді Kaspersky мамандары қалыптастырады және үнемі жаңартып отырады.
  - Microsoft бағдарламаларынан басқа үшінші тарап бағдарламаларындағы осалдықтарды түзету.

Кезеңдер

Осалдықтарды анықтау және түзету келесі кезеңдерден тұрады:

1. **Басқарылатын құрылғыларда орнатылған бағдарламалық жасақтамадағы осалдықтарды іздеу**

   Басқарылатын құрылғыларда орнатылған бағдарламалардағы осалдықтарды табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосыңыз. Бұл тапсырма аяқталғаннан кейін, Kaspersky Security Center бағдарламасы құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап бағдарламалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады.

   Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, оны қазір іске қосыңыз немесе тапсырманы қолмен жасаңыз.

   Нұсқаулар:

   - Басқару консолі: Бағдарламаларда осалдықтарды іздеу, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін кестені белгілеу.
   - Kaspersky Security Center Web Console: Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы параметрлері.

2. **Анықталған бағдарламалық жасақтама осалдықтары тізімін талдау**

   Бағдарламалық жасақтама осалдықтары тізімін қарап, қандай осалдықтарды түзету керектігін шешіңіз. Әрбір осалдық туралы толық ақпаратты көру үшін тізімдегі осалдық атауын басыңыз. Тізімдегі әрбір осалдық үшін басқарылатын құрылғылардағы осалдық статистикасын да көруге болады.

   Нұсқаулар:

   - Басқару консолі: Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау, Басқарылатын құрылғылардағы осалдықтар статистикасын қарау.
   - Kaspersky Security Center Web Console: Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау, Басқарылатын құрылғылардағы осалдықтар статистикасын қарау.

3. **Осалдықты түзетуді конфигурациялау**

   Бағдарламаларда осалдықтарды анықтап, сіз *Қажетті жаңартуларды орнату және осалдықтарды түзету* немесе *Осалдықтарды түзету* тапсырмасын қолдану арқылы басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын түзете аласыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, үшінші тарап бағдарламаларында, соның ішінде басқарылатын құрылғыларға орнатылған Microsoft бағдарламаларында жаңарту және осалдықтарды түзету үшін қолданылады. Бұл тапсырма бірнеше жаңартуларды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықтарды түзетуге мүмкіндік береді. Назар аударыңыз, Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана осы тапсырманы жасауға болады. Бағдарламалық жасақтама осалдықтарын түзету үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы ұсынылған бағдарламалық жасақтама жаңартуларын қолданады.

Осалдықтарды түзету тапсырмасы Осалдықтар мен патчтарды басқару үшін лицензияны қажет етпейді. Бұл тапсырманы пайдалану мақсатында, тапсырма параметрлерінде көрсетілген үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін пайдаланушылық түзетулерді қолмен көрсету қажет. *Осалдықтарды түзету* тапсырмасы үшінші тарап бағдарламалары үшін ұсынылған Microsoft бағдарламаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады.

Сіз осы тапсырмалардың бірін автоматты түрде жасайтын осалдықтарды түзету шеберін іске қоса аласыз немесе сол тапсырмалардың бірін қолмен жасай аласыз.

Нұсқаулар:

- Басқару консолі: Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушылық түзетулер, Бағдарламалық жасақтама осалдықтарын түзету.
- Kaspersky Security Center Web Console: Үшінші тарап бағдарламаларындағы осалдықтар үшін пайдаланушылық түзетулер, Үшінші тарап бағдарламаларындағы осалдықтарды түзету, Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау.

4 Тапсырманың кестесін белгілеу

Осалдықтар тізімі әрқашан өзекті екеніне көз жеткізу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының іске қосылу кестесін белгілеңіз, сонда ол мезгіл-мезгіл автоматты түрде іске қосылады. Ұсынылатын орташа кезең – аптасына бір рет.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, оны іске қосуды *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасына арналған жиілікпен немесе одан сирек жиілікпен іске қосуды белгілей аласыз. *Осалдықтарды түзету* тапсырмасының кестесін белгілеген кезде, тапсырманы іске қоспас бұрын Microsoft бағдарламаларының түзетулерін таңдау немесе үшінші тарап бағдарламалары үшін арнайы түзетулерді көрсету керек.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5 Бағдарламалық жасақтама осалдықтарын елемеу (қажет болса)

Барлық басқарылатын құрылғыларда немесе тек таңдалған басқарылатын құрылғыларда түзетілуі тиісті бағдарламалардағы осалдықты елемеуге болады.

Нұсқаулар:

- Басқару консолі: Бағдарламалардағы осалдықтарды елемеу.
- Kaspersky Security Center Web Console: Бағдарламалық жасақтама осалдықтарын елемеу.

6 Осалдықтарды түзету тапсырмасын іске қосу

Қажетті жаңартуларды орнату және осалдықтарды түзету немесе *Осалдықты түзету* тапсырмасын іске қосыңыз. Тапсырма аяқталғаннан кейін, оның тапсырмалар тізімінде *Сәтті аяқталды* күйі бар екеніне көз жеткізіңіз.

7 Бағдарламалық жасақтама осалдықтарын түзету нәтижелері туралы есеп жасау (қажет болса)

Жабық осалдықтар туралы статистиканы көру үшін осалдықтар туралы есепті жасаңыз. Есепте түзетілмеген бағдарламалық жасақтама осалдықтары туралы ақпарат көрсетіледі. Осылайша, сіз өзіңіздің ұйымыңыздағы үшінші тарап бағдарламаларындағы, соның ішінде Microsoft бағдарламалық жасақтамасындағы осалдықтарды анықтау және түзету туралы түсінікке ие бола аласыз.

Нұсқаулар:

- Басқару консолі: Есепті жасау және қарау
- Kaspersky Security Center Web Console: Есепті жасау және қарау

8. **Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету параметрлерін тексеру**

   Келесіні орындағаныңызға көз жеткізіңіз:

   - басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтары тізімін тауып, қарап шыққаныңызға;
   - егер қаласаңыз, бағдарламалардағы осалдықтарды елемегеніңізге;
   - осалдықты түзету тапсырмасын конфигурациялағаныңызға;
   - бағдарламалардағы осалдықтарды іздеуге және түзетуге арналған тапсырмаларды дәйекті түрде іске қосылатындай етіп іске қосуды жоспарлады;
   - осалдықтарды түзету міндеті іске қосылғанын тексерді.

Нәтижелер

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасасаңыз және конфигурацияласаңыз, осалдықтар басқарылатын құрылғыларда автоматты түрде жабылады. Тапсырманы іске қосу кезінде тапсырма қолжетімді бағдарламалық жасақтама жаңартуларының тізімін тапсырма параметрлерінде көрсетілген ережелермен салыстырады. Ережелердегі критерийлерге сәйкес келетін барлық бағдарламалық жасақтама жаңартулары Басқару сервері қоймасына жүктеледі және бағдарламалардағы осалдықтарды түзету үшін орнатылады.

Осалдықтарды түзету тапсырмасын жасаған болсаңыз, Microsoft бағдарламаларындағы осалдықтар ғана түзетіледі.

Бағдарламалық жасақтама осалдықтарын анықтау және түзету туралы

Kaspersky Security Center бағдарламасы Microsoft Windows операциялық жүйелерінің басқаруымен жұмыс істейтін басқарылатын құрылғылардағы бағдарламаларда осалдықтарды анықтайды және түзетеді. Осалдықтар операциялық жүйелерде және Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламаларында кездеседі.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Бағдарламалық жасақтама осалдықтарын анықтау

Осалдықтарды анықтау үшін Kaspersky Security Center бағдарламасы белгілі осалдықтар туралы дерекқордағы белгілерге негізделген бағдарламалық жасақтаманың белгілі осалдықтарын іздейді. Бұл дерекқорды Kaspersky мамандары қалыптастырады. Онда осалдықтардың сипаттамасы, осалдықтарды анықтау күні, осалдықтардың қауіптілік деңгейі сияқты осалдықтар туралы ақпарат бар. Сіз осалдықтар туралы мәліметті Kaspersky сайтынан ала аласыз.

Kaspersky Security Center бағдарламасында бағдарламалардың осалдықтардың іздеу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы қолданылады.

Кейбір жағдайларда Microsoft Windows операциялық жүйесінде анықталған осалдықтарды келесі тәсілдердің бірі арқылы жоюға болады:

- Операциялық жүйе үшін жаңартуларды орнатыңыз.
- Операциялық жүйені жаңа нұсқаға жаңартыңыз (мысалы, Windows 10-дан Windows 11-ге дейін).

Бұл сценарийде Kaspersky Security Center бірдей осалдық үшін екі жазбаны көрсетеді.

Бағдарламаларда осалдықты түзету

Бағдарламаларда осалдықтарды түзету үшін, Kaspersky Security Center бағдарламасы бағдарламалық жасақтама өндірушілері шығарған бағдарламалық жасақтама жаңартуларын қолданады. Бағдарламалық жасақтаманы жаңарту метадеректері келесі тапсырмаларды орындау нәтижесінде Басқару сервері қоймасына жүктеледі:

- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*. Бұл тапсырма Kaspersky бағдарламалары мен үшінші тарап бағдарламалары үшін жаңарту метадеректерін жүктеуге арналған. Бұл тапсырма Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолмен жасауға болады.
- *Windows Update жаңартуларын синхрондау*. Бұл тапсырма Microsoft бағдарламалық жасақтамасының жаңартуларының метадеректерін жүктеуге арналған.

Осалдықтарды түзетуге арналған бағдарламалық жасақтаманың жаңартулары толық дистрибутивтер немесе патчтар түрінде ұсынылуы мүмкін. Бағдарламалық жасақтаманың осалдықтарын түзететін бағдарламалық жасақтама жаңартулары *түзетулер* деп аталады. *Ұсынылған түзетулер* – бұл Kaspersky мамандары орнатуға ұсынатын түзетулер. *Пайдаланушылық түзетулер* – бұл пайдаланушылар орнату үшін қолмен көрсетілетін түзетулер. Пайдаланушылық түзетулерді орнату үшін осы түзетуді қамтитын орнату пакетін жасау керек.

Kaspersky Security Center лицензиясы Осалдықтар мен патчтарды басқару мүмкіндіктерін көздесе, осалдықтарды түзету үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын пайдаланыңыз. Бұл тапсырма ұсынылған түзетулерді орнату арқылы бірнеше осалдықтарды автоматты түрде түзетеді. Бұл тапсырма үшін бірнеше осалдықтарды түзету үшін белгілі бір ережелерді қолмен конфигурациялауға болады.

Kaspersky Security Center лицензиясы Осалдықтар мен патчтарды басқару мүмкіндіктерін көздемесе, осалдықтарды түзету үшін *Осалдықтарды түзету* тапсырмасын пайдаланыңыз. Бұл тапсырманың көмегімен Microsoft бағдарламалары үшін ұсынылған түзетулерді және үшінші тарап бағдарламалары үшін пайдаланушылық түзетулерді орнату арқылы осалдықтарды түзетуге болады.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап бағдарламалық жасақтамасы жаңартулары Kaspersky технологиялары арқылы зиянды БҚ-дың бар-жоғы тұрғысынан автоматты түрде тексеріледі. Бұл технологиялар файлдарды автоматты түрде тексеру үшін қолданылады және антивирустық тексеруді, статикалық талдауды, динамикалық талдауды, "құмсалғыштың" жүріс-тұрысын талдауды және машиналық оқытуды қамтиды.

Kaspersky мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап бағдарламалық жасақтамасы жаңартуларын қолмен талдамайды. Сонымен қатар Kaspersky мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Бағдарламалық жасақтаманың кейбір осалдықтарын түзету үшін, қажет болса, бағдарламалық жасақтаманы орнатуға арналған лицензиялық келісімді қабылдау керек. Егер сіз Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтаманың осалдығы түзетілмейді.

Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау

Клиент құрылғыларында табылған осалдықтар тізімін көру үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама осалдықтары** салынған қалтасын таңдаңыз.

   Басқарылатын құрылғыларда табылған бағдарламалардағы осалдықтар тізімі бар бет көрсетіледі.

Таңдалған осалдық туралы ақпарат алу үшін:

1. Осалдықтың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

Осалдық сипаттары терезесі ашылып, онда келесі ақпарат көрсетіледі:

- осалдық анықталған бағдарлама;
- осалдық анықталған құрылғылардың тізімі;
- осалдықты түзету туралы ақпарат.

Барлық анықталған осалдықтар туралы есепті қарау үшін:

1. **Бағдарламалық жасақтама осалдықтары** қалтасында **Осалдықтар туралы есепті көру** сілтемесінен өтіңіз.

   Құрылғыларда орнатылған бағдарламалардағы осалдықтар туралы есеп жасалады. Есепті **Есептер** қойыншасында қажетті Басқару серверінің аты бар түйінде көруге болады.

Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау

Басқарылатын құрылғылардағы бағдарламалардағы әрбір осалдықтың статистикалық ақпаратын көруге болады. Статистика диаграммалар түрінде ұсынылған. Диаграмма келесі күйлері бар құрылғылардың санын көрсетеді:

- *Еленбеген: <құрылғылар саны>*. Егер сіз осалдық сипаттарында осалдықты елемеу параметрін қолмен орнатсаңыз, осы күй тағайындалады.
- *Түзетілген: <құрылғылар саны>*. Егер осалдықты түзету тапсырмасы сәтті аяқталса, осы күй белгіленеді.
- *Түзетуге жоспарланған: <құрылғылар саны>* Егер сіз осалдықтарды түзету тапсырмасын жасаған болсаңыз, бірақ тапсырма әлі аяқталмаған болса, осы күй белгіленеді.
- *Патч қолданылған: <құрылғылардың саны>*. Егер сіз осалдықты түзету үшін бағдарламалық жасақтаманы жаңартуды қолмен таңдаған болсаңыз, осы күй тағайындалады, бірақ бұл жаңарту осалдықты түзетпеді.
- *Түзету қажет: <құрылғылар саны>*. Осалдық кейбір басқарылатын құрылғыларда ғана жабылған болса, бірақ басқа басқарылатын құрылғыларда осалдықты түзету қажет болса, осы күй тағайындалады.

Басқарылатын құрылғылардағы осалдық статистикасын көру үшін:

1. Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама осалдықтары** салынған қалтасын таңдаңыз.

   Басқарылатын құрылғыларда табылған бағдарламалардағы осалдықтар тізімі бар бет көрсетіледі.

2. Статистикасын көргіңіз келетін осалдықты таңдаңыз.

   Таңдалған нысанмен жұмыс істеуге арналған блокта осалдық күйлерінің диаграммасы көрсетіледі. Күйді басу арқылы, осалдықтың таңдалған күйі бар құрылғылардың тізімі ашылады.

Бағдарламалық жасақтама осалдықтарын іздеу

Бағдарламаны жылдам іске қосу шебері көмегімен бағдарламаны конфигурациялаған болсаңыз, *Осалдықтарды іздеу* тапсырмасы автоматты түрде жасалады. Тапсырманы **Басқарылатын құрылғылар** қалтасында, **Тапсырмалар** қойыншасында қарауға болады.

Клиент құрылғыларында орнатылған бағдарламаларда осалдықтарды іздеу тапсырмасын жасау:

1. Консоль ағашында **Кеңейтілген → Бағдарламаларды басқару**, содан соң **Бағдарламалық жасақтама осалдықтары** ішкі қалтасын таңдаңыз.
2. Жұмыс аймағында **Қосымша әрекеттер → Осалдықтарды сканерлеуді конфигурациялау** тармағын таңдаңыз.

   Осалдықтарды іздеуге арналған тапсырма бұрыннан бар болса, ол **Басқарылатын құрылғылар** қалтасындағы **Тапсырмалар** қойыншасында, бұрыннан бар таңдалған тапсырмалармен бірге көрсетіледі. Әйтпесе, осалдықтарды және қажетті жаңартуларды табу тапсырмасын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. **Тапсырма түрін таңдау** терезесінде **Осалдықтарды және қажетті жаңартуларды іздеу** тармағын таңдаңыз.

4. **Параметрлер** шеңбері терезесінде тапсырманың келесі тапсырмаларын көрсетіңіз:

- **Microsoft тізіміндегі осалдықтар мен жаңартуларды іздеңіз**

  Осалдықтар мен жаңартуларды іздеу кезінде Kaspersky Security Center бағдарламасы ағымдағы сәтте қолжетімді Microsoft жаңартулардың көздерінен Microsoft қолжетімді жаңартулары туралы деректерді қолданады.

  Мысалы, Microsoft жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

  - **Деректерді жаңарту үшін жаңарту серверіне қосылу**

    Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

    - Kaspersky Security Center Басқару сервері (Желілік агент саясатының параметрлерін қараңыз).
    - Ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server.
    - Microsoft жаңарту серверлері.

    Егер бұл параметр қосулы болса, басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылып, Microsoft Windows қолжетімді жаңартулары туралы ақпарат алады.

    Егер бұл параметр өшірулі болса, басқарылатын құрылғыдағы Windows Update агенті бұған дейін Microsoft жаңарту көзінен алған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты пайдаланады.

    Microsoft жаңарту көзіне қосылу ресурстарды қажет етуі мүмкін. Егер сіз осы жаңарту көзіне басқа тапсырмада немесе Желілік агент саясатының сипаттарында, **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** бөлімінде тұрақты қосылым орнатқан болсаңыз, бұл параметрді өшіре аласыз Егер сіз бұл параметрді өшіргіңіз келмесе, Серверге түсетін жүктемені азайту үшін тапсырмалар кестесін 360 минут аралығындағы тапсырманы іске қосу кідірісінің кездейсоқ мәнін пайдалануға болатындай конфигурациялауға болады.

    Әдепкі бойынша, параметр қосулы.

Желілік агент саясаты параметрлерінің келесі мәндерінің тіркесімі жаңартуларды алу режимін анықтайды:

- Басқарылатын құрылғыдағы Windows Update агенті жаңартуларды алу үшін жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының сипаттарында қосылған және **Windows Update жаңартуларын іздеу режимі** параметрі желілік агент саясатының параметрлерінде **Белсенді** болып белгіленген жағдайда ғана қосылады.

- *Осалдықты сканерлеу* тапсырмасын орындаған кезде Microsoft Windows жаңарту көзіне қосылымды бастау және жаңартуларды жүктеп алу үшін Желілік агент қажет болмаса, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатуға болады, бұл арада **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы күйде қала беруі керек. Бұл, ресурстарды үнемдеуге және осалдықтарды іздеу үшін бұрын алынған Windows жаңартуларын пайдалануға мүмкіндік береді. Microsoft Windows жаңартуларын алуды басқа тәсілмен конфигурациялаған болсаңыз, пассивті режимді пайдалануға болады. Microsoft Windows жаңартуларын басқа жолмен алу үшін конфигурацияланбасаңыз, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатпаңыз, себебі бұл жағдайда жаңартулар туралы ақпарат ешқашан алынбайды.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметріне қарамастан (қосулы немесе өшірулі), егер **Windows Update жаңартуларын іздеу режимі** параметрі үшін **Өшірулі** параметрлер тобында таңдалса, онда Kaspersky Security Center бағдарламасы жаңартулар туралы ақпаратты сұрамайды.

- **Kaspersky ұсынған үшінші тарап осалдықтары мен жаңартуларын іздеңіз**

  Егер бұл параметр қосулы болса, Kaspersky Security Center бағдарламасы Windows тізімдемесінде және **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз** бөлімінде көрсетілген қалталарда үшінші тарап өндірушілерінің бағдарламалары (Kaspersky және Microsoft-тан басқа өндірушілер шығарған бағдарламалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап бағдарламаларының толық тізімін Kaspersky бақылайды.

  Егер бұл параметр өшірулі болса, Kaspersky Security Center бағдарламасы үшінші тарап бағдарламалары үшін осалдықтар мен қажетті жаңартуларды іздемейді. Мысалы, Microsoft Windows жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

- **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз**

  Kaspersky Security Center бағдарламасы осалдықтарды түзетуді және жаңартуларды орнатуды қажет ететін үшінші тарап бағдарламаларын іздейтін қалталар. Жүйе айнымалыларын пайдалануға болады.

  Бағдарламалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген бағдарламалар орнатылған жүйелік қалталар бар.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

5. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

   - **Кесте бойынша іске қосу:**

     Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

     - **N сағат сайын**

       Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

     - **N күн сайын**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

     - **N апта сайын**

       Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **N минут сайын**

       Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

       Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

     - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

       Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

       Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Қоймаға жаңартуларды жүктеу кезінде**

  Бұл тапсырма жаңартуларды қоймаға жүктегеннен кейін іске қосылады. Мысалы, сізге осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін осы кесте қажет болуы мүмкін.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

6. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

7. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

   Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы нәтижесінде, тапсырмалар тізімінде, **Басқарылатын құрылғылар** қалтасында, **Тапсырмалар** қойыншасында көрсетілетін **Осалдықтарды және қажетті жаңартуларды іздеу** тапсырмасы жасалады.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы аяқталған кезде, Басқару сервері құрылғыда орнатылған бағдарламаларда кездесетін осалдықтардың тізімін көрсетеді; сонымен қатар Сервер анықталған осалдықтарды түзету үшін қажетті барлық бағдарламалық жасақтама жаңартуларын көрсетеді.

Егер 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" қатесі көрсетілсе, бұл мәселені Windows тізімдемесі арқылы шешуге болады.

Басқару сервері екі тапсырманы дәйекті түрде іске қосқан кезде қажетті бағдарламалық жасақтама жаңартуларының тізімін көрсетпейді: **Жедел орнату файлдарын жүктеп алу** параметрі өшірілген *Windows Update жаңартуларын синхрондау* тапсырмалары, содан кейін *Осалдықтар мен қажетті жаңартуларды іздеу* тапсырмалары. Қажетті бағдарламалық жасақтама жаңартуларының тізімін көру үшін *Осалдықтар мен қажетті жаңартуларды іздеу* тапсырмасын қайтадан іске қосу керек.

Желілік агент Windows және басқа Microsoft бағдарламаларының кез келген жаңартулары туралы ақпаратты Windows Update-тен немесе Басқару сервері WSUS сервері рөлін атқаратын болса, Басқару серверінен алады. Ақпарат, бағдарламаларды іске қосу кезінде (егер бұл саясатта қарастырылған болса) және клиент құрылғыларындағы *Осалдықтар мен қажетті жаңартуларды іздеу* тапсырмасын іске қосқан сайын беріледі.

Бағдарламаларда осалдықты түзету

Жылдам іске қосу шеберінің **Жаңартуларды басқару параметрлері** бетінде **Қажетті жаңартуларды іздеу және орнату** опциясын таңдасаңыз, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы автоматты түрде жасалады. Тапсырма **Басқарылатын құрылғылар** қалтасында, **Тапсырмалар** қойыншасында көрсетіледі.

Әйтпесе, сіз келесі әрекеттердің бірін орындай аласыз:

- Қолжетімді жаңартуларды орнату арқылы осалдықтарды түзету тапсырмасын жасаңыз.
- Қолданыстағы осалдықтарды түзету тапсырмасына осалдықтарды түзету ережесін қосыңыз.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Осалдықтарды түзету тапсырмасы арқылы осалдықтарды түзету

Сіз келесі әрекеттердің бірін орындай аласыз:

- Белгілі бір ережелерге сәйкес келетін бірнеше осалдықтарды түзету тапсырмасын жасаңыз.
- Осалдықты таңдап, оны түзету және ұқсас осалдықтарды түзету үшін тапсырма жасаңыз.

Белгілі бір ережелерге сәйкес келетін осалдықтарды түзету үшін:

1. Консоль ағашында құрылғылардағы осалдықтарды түзеткіңіз келетін Басқару серверін таңдаңыз.
2. Бағдарламаның басты терезесінің **Көру** мәзірінде **Интерфейсті конфигурациялау** тармағын таңдаңыз.
3. Ашылған терезеде **Осалдықтар мен патчтарды басқаруды көрсету** жалаушасын қойып, **OK** түймесін басыңыз.
4. Бағдарлама хабары бар терезеде **OK** түймесін басыңыз.
5. Өзгерістер күшіне енуі үшін Басқару консолін қайта іске қосыңыз.
6. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
7. Жұмыс аймағында **Тапсырмалар** қойыншасын таңдаңыз.
8. **Тапсырма жасау** түймесі арқылы жаңа тапсырма жасау шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.
9. Жаңа тапсырма жасау шеберінің **Тапсырма түрін таңдау** терезесінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тармағын таңдаңыз.

   Тапсырма көрсетілмесе, есептік жазбада **Жүйені басқару**: **Осалдықтар мен патчтарды басқару** функционалды аймағына арналған **Оқу**, **өзгерту** және **орындау** құқықтары бар екенін тексеріңіз. Сіз осы қатынас құқықтарынсыз *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасай алмайсыз және конфигурациялай алмайсыз.
10. **Параметрлер** шеңбері терезесінде тапсырманың келесі тапсырмаларын көрсетіңіз:

    - **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз**

      Бұл ережелер клиент құрылғыларына жаңартуларды орнату кезінде қолданылады. Егер ережелер көрсетілмесе, тапсырма орындалмайды. Ережелермен жұмыс істеу туралы қосымша ақпаратты Жаңартуларды орнату ережелері бөлімінен қараңыз.

    - **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау**

      Егер жалауша қойылса, құрылғыны қайта іске қоспас немесе өшірмес бұрын жаңартуды орнату орындалады. Әйтпесе, жаңартуларды орнату кесте бойынша жүзеге асырылады.

      Жаңартуларды орнату құрылғылардың жұмысына әсер етуі мүмкін болса, осы жалаушаны қойыңыз.

      Әдепкі бойынша, параметр өшірулі.

- **Қажетті жалпы жүйелік құрамдастарды орнату**

  Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

  Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартулар кезінде бағдарламаның жаңа нұсқаларын орнатуға рұқсат ету**

  Бұл опция қосылған болса, бағдарламалық жасақтама қолданбасының жаңа нұсқасын орнатуға әкелсе, жаңартуларға рұқсат беріледі.

  Бұл параметр өшірулі болса, бағдарлама жаңартылмайды. Бағдарламалардың жаңа нұсқаларын кейінірек қолмен немесе басқа тапсырманы қолдана отырып, орнатуға болады. Мысалы, егер сіздің компанияңыздың инфрақұрылымы бағдарламаның жаңа нұсқасын қолдамаса немесе сынақ инфрақұрылымындағы жаңартуды тексеру қажет болса, бұл параметрді пайдалануға болады.

  Әдепкі бойынша, параметр қосулы.

  > Бағдарламаның жаңа нұсқасын орнатқаннан кейін, клиент құрылғыларында орнатылған және жаңартылатын бағдарламаның жұмысына байланысты басқа бағдарламалардың жұмысы бұзылуы мүмкін.

- **Жаңартуларды құрылғыға орнатпастан жүктеп алу**

  Егер жалауша қойылса, бағдарлама жаңартуларды құрылғыға жүктейді, бірақ оларды автоматты түрде орнатпайды. Содан кейін, жүктелген жаңартуларды қолмен орнатуға болады.

  Microsoft жаңартулары Windows қызметтік қалтасына жүктеледі. Үшінші тарап бағдарламаларының жаңартулары (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) **Жаңартуларды келесі жерге жүктеп алу** өрісінде көрсетілген қалтаға жүктеледі.

  Егер бұл параметр өшірулі болса, жаңартулар құрылғыға автоматты түрде орнатылады.

  Әдепкі бойынша, параметр өшірулі.

  - **Жаңартуларды келесі жерге жүктеп алу**

    Бұл қалта, үшінші тарап бағдарламаларының (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) жаңартуларын жүктеу үшін қолданылады.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

11. **Операциялық жүйені қайта іске қосу опциясын таңдау** шебері терезесінде операциядан кейін клиент құрылғыларындағы операциялық жүйені қайта қосу қажет болса, орындалатын әрекетті таңдаңыз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Келесі уақыттан кейін қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

Әдепкі бойынша, параметр өшірулі.

12. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

    - **Кесте бойынша іске қосу:**

      Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

      - **N сағат сайын**

        Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

        Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

      - **N күн сайын**

        Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

        Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

      - **N апта сайын**

        Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

        Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

      - **N минут сайын**

        Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

        Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

      - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

        Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

        Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

        Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

      - **Апта сайын**

        Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

- Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
- Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

  Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
- Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

13. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

14. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

    Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы нәтижесінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасы жасалып, **Тапсырмалар** қалтасында көрсетіледі.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Тапсырманың нәтижелерінде 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" қатесі бар болса, бұл мәселені Windows тізімдемесі арқылы шешуге болады.

Қажетті және оған ұқсас осалдықты түзету үшін:

1. Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама осалдықтары** салынған қалтасын таңдаңыз.

2. Түзеткіңіз келетін осалдықты таңдаңыз.

3. **Осалдықтарды түзету шеберін іске қосу** түймесін басыңыз.

   Осалдықтарды түзету шебері ашылады.

   Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері функционалы қолжетімді болады.

   Содан кейін, шебердің нұсқауларын орындаңыз.

4. **Осалдықты түзету бойынша бар тапсырмаларды іздеу** бөлімінде келесі параметрлерді көрсетіңіз:

   - **Осы осалдықты түзететін тапсырмаларды ғана көрсету**

     Егер бұл параметр қосулы болса, осалдықты түзету шебері таңдалған осалдықты түзету үшін бар тапсырмаларды іздейді.

     Егер бұл параметр өшірулі болса немесе қолданылатын тапсырмалар табылмаса, осалдықты түзету шебері осалдықты түзету үшін ереже немесе тапсырма жасауды ұсынады.

     Әдепкі бойынша, параметр қосулы.

   - **Осы осалдықты түзететін жаңартуларды растау**

     Осалдықты түзететін жаңартулар орнатуға мақұлданады. Жаңартуларды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, осы параметрді қосыңыз.

     Әдепкі бойынша, параметр өшірулі.

5. Егер сіз осалдықты түзету үшін бар тапсырмаларды іздеуді таңдасаңыз және бірнеше тапсырмалар табылса, сол тапсырмалардың сипаттарын көруге немесе оларды қолмен іске қосуға болады. Қосымша әрекеттер қажет емес.

   Әйтпесе, **Жаңа осалдықты түзету тапсырмасы** түймесін басыңыз.

6. Бар тапсырмаға қосу үшін осалдықты түзететін ереже түрін таңдап, **Дайын** түймесін басыңыз.

7. Бағдарламаның барлық алдыңғы нұсқаларын орнату терезесі ашылады. Таңдалған жаңартуларды орнату үшін қажет болса, бағдарлама нұсқаларын дәйекті түрде орнатуға келіссеңіз, **Иә** түймесін басыңыз. Егер сіз нұсқаларды дәйекті түрде орнатпай, бағдарламаны тікелей жаңартқыңыз келсе, **Жоқ** түймесін басыңыз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

   Жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау шебері ашылады. Содан кейін, шебердің нұсқауларын орындаңыз.

8. **Операциялық жүйені қайта іске қосу опциясын таңдау** шебері терезесінде операциядан кейін клиент құрылғыларындағы операциялық жүйені қайта қосу қажет болса, орындалатын әрекетті таңдаңыз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

   - **Құрылғыны қайта іске қосу**

     Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

   - **Пайдаланушыдан әрекетті орындауды сұрау**

     Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

     - **Сұрауды қайталау жиілігі (мин)**

       Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

       Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

     - **Келесі уақыттан кейін қайта іске қосу (мин)**

       Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

   - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

     Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

     Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

     Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

     Әдепкі бойынша, параметр өшірулі.

9. Шебердің **Тапсырма белгіленетін құрылғыларды таңдау** бетінде келесі нұсқалардың бірін таңдаңыз:

   - **Басқару серверімен анықталған желілік құрылғыларды таңдау**

     Бұл жағдайда, тапсырма арнайы құрылғыларға тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

     Мысалы, сіз бұл параметрді Желілік агентті тағайындалмаған құрылғыларға орнату тапсырмасында пайдалана аласыз.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

     Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

10. Шебердің **Тапсырма кестесін конфигурациялау** бетінде тапсырманы іске қосу кестесін құрастыруға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

    - **Кесте бойынша іске қосу:**

      Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

      - **N сағат сайын**

        Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

        Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

      - **N күн сайын**

        Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

        Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N апта сайын**

  Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

  Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

  Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

11. Шебердің **Тапсырма атауын анықтау** бетінде, жасалатын тапсырманың атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

12. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

    Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Шебердің жұмысы нәтижесінде **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасы жасалып, **Тапсырмалар** қалтасында көрсетіледі.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Қолданыстағы осалдықтарды түзету тапсырмасына ереже қосу арқылы осалдықты түзету

Қолданыстағы осалдықтарды түзету тапсырмасына ереже қосу арқылы осалдықты түзету үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама осалдықтары** салынған қалтасын таңдаңыз.

2. Түзеткіңіз келетін осалдықты таңдаңыз.

3. **Осалдықтарды түзету шеберін іске қосу** түймесін басыңыз.

   Осалдықтарды түзету шебері ашылады.

   Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері функционалы қолжетімді болады.

   Содан кейін, шебердің нұсқауларын орындаңыз.

4. **Осалдықты түзету бойынша бар тапсырмаларды іздеу** бөлімінде келесі параметрлерді көрсетіңіз:

   - **Осы осалдықты түзететін тапсырмаларды ғана көрсету**

     Егер бұл параметр қосулы болса, осалдықты түзету шебері таңдалған осалдықты түзету үшін бар тапсырмаларды іздейді.

     Егер бұл параметр өшірулі болса немесе қолданылатын тапсырмалар табылмаса, осалдықты түзету шебері осалдықты түзету үшін ереже немесе тапсырма жасауды ұсынады.

     Әдепкі бойынша, параметр қосулы.

   - **Осы осалдықты түзететін жаңартуларды растау**

     Осалдықты түзететін жаңартулар орнатуға мақұлданады. Жаңартуларды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, осы параметрді қосыңыз.

     Әдепкі бойынша, параметр өшірулі.

5. Егер сіз осалдықты түзету үшін бар тапсырмаларды іздеуді таңдасаңыз және бірнеше тапсырмалар табылса, сол тапсырмалардың сипаттарын көруге немесе оларды қолмен іске қосуға болады. Қосымша әрекеттер қажет емес.

   Әйтпесе, **Бар тапсырмаға осалдықты түзету ережесін қосу** түймесін басыңыз.

6. Ереже қосқыңыз келетін тапсырманы таңдап, **Ереже қосу** түймесін басыңыз.

   Сондай-ақ, бұрыннан бар тапсырмалардың сипаттарын көруге, оларды қолмен іске қосуға немесе тапсырма жасауға болады.

7. Таңдалған тапсырмаға қосу үшін ереже түрін таңдап, **Дайын** түймесін басыңыз.

8. Бағдарламаның барлық алдыңғы нұсқаларын орнату терезесі ашылады. Таңдалған жаңартуларды орнату үшін қажет болса, бағдарлама нұсқаларын дәйекті түрде орнатуға келіссеңіз, **Иә** түймесін басыңыз. Егер сіз нұсқаларды дәйекті түрде орнатпай, бағдарламаны тікелей жаңартқыңыз келсе, **Жоқ** түймесін басыңыз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

Осалдықты түзетуге арналған жаңа ереже бұрыннан бар **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырмасына қосылған.

Оқшауланған желіде осалдықтарды түзету

Бұл бөлімде Басқару серверлеріне қосылған және интернетке қатынасу мүмкіндігі жоқ басқарылатын құрылғылардағы үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін қолдануға болатын әрекеттер сипатталған.

Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету

Жаңартуларды орнатуға және оқшауланған желідегі басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларының осалдықтарын түзетуге болады. Мұндай желілерге, интернетке қатынаса алмайтын Басқару серверлері мен оларға қосылған басқарылатын құрылғылар жатады. Мұндай желідегі осалдықтарды түзету үшін интернетке қосылған Басқару сервері қажет. Сондай-ақ, сіз патчтарды (қажетті жаңартуларды) интернетке қосылған Басқару серверінің көмегімен жүктей аласыз және патчтарды оқшауланған Басқару серверлеріне жібере аласыз.

Сіз бағдарламалық жасақтама өндірушілері шығарған үшінші тарап бағдарламалық жасақтамасының жаңартуларын жүктей аласыз, бірақ Microsoft бағдарламалық жасақтамасының жаңартуларын Kaspersky Security Center көмегімен оқшауланған Басқару серверлерінде жүктей алмайсыз.

Оқшауланған желіде осалдықтарды түзету процесінің қалай жұмыс істейтінін білу үшін осы процестің сипаттамасы және схемасымен танысыңыз.

Алдын ала талаптар

Бастамас бұрын келесі әрекеттерді орындаңыз:

1. Интернетке қосылу және түзетулерді жүктеу үшін бір құрылғыны бөлектеңіз. Бұл құрылғы интернетке қатынасу мүмкіндігі бар Басқару сервері болып саналады.
2. Келесі құрылғыларда Kaspersky Security Center бағдарламасының кемінде 14 нұсқасын орнатыңыз:
   - Интернетке қатынасу мүмкіндігі бар Басқару сервері ретінде әрекет ететін бөлектелген құрылғы.
   - Интернеттен оқшауланған Басқару серверлері (бұдан әрі – оқшауланған Басқару серверлері) рөлін атқаратын оқшауланған құрылғылар.
3. Әрбір Басқару серверінде жаңартулар мен түзетулерді жүктеп алу және сақтау үшін дискіде жеткілікті орын бар екеніне көз жеткізіңіз.

Кезеңдер

Оқшауланған Басқару серверлеріне қатысты басқарылатын құрылғыларда жаңартуларды орнату және үшінші тарап бағдарламаларының осалдықтарын түзету келесі қадамдардан тұрады:

1. **Интернетке қатынасу арқылы Басқару серверін конфигурациялау**

   Үшінші тарап бағдарламалық жасақтамасының қажетті жаңартуларына сұрауларды өңдеу және жүктеп алу үшін интернетке қатынасу рұқсаты бар Басқару серверін дайындаңыз.

2. **Оқшауланған Басқару серверлерін конфигурациялау**

   Оқшауланған Басқару серверлері үнемі қажетті жаңартулар тізімдерін құрастырып, интернетке қатынаса алатын Басқару сервері жүктейтін патчтарды өңдей алуы үшін осы оқшауланған Басқару серверлерін дайындаңыз. Конфигурациялаудан кейін, оқшауланған Басқару серверлері интернеттен патчтарды жүктеуге тырыспайды. Мұның орнына, олар патчтар арқылы жаңартуларды алады.

3 Оқшауланған Басқару серверлеріне патчтарды беру және жаңартуларды орнату

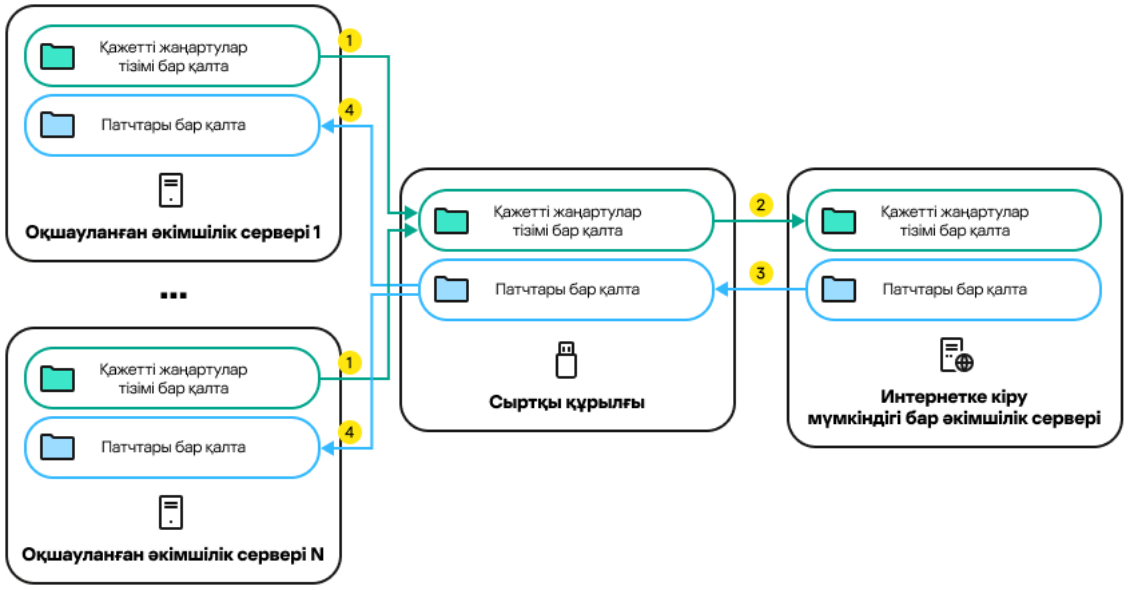
Басқару серверлерін конфигурациялауды аяқтағаннан кейін, сіз интернетке қатынасатын Басқару сервері мен оқшауланған Басқару серверлері арасында қажетті жаңартулар мен патчтар тізімдерін жібере аласыз. Әрі қарай, түзетулерден алынған жаңартулар *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы арқылы басқарылатын құрылғыларға орнатылады.

Нәтижелер

Осылайша, үшінші тарап бағдарламаларының жаңартулары оқшауланған Басқару серверлеріне беріледі және қосылған басқарылатын құрылғыларға Kaspersky Security Center көмегімен орнатылады. Өзіңізге қажетті жиілікпен, мысалы, күніне бір немесе бірнеше рет жаңартуларды алып тұру үшін Басқару серверлерін бір рет конфигурациялау жеткілікті.

Оқшауланған желідегі үшінші тарап бағдарламаларының осалдықтарын түзету туралы

Оқшауланған желідегі үшінші тарап бағдарламаларындағы осалдықтарды түзету процесі суретте көрсетілген және төменде сипатталған. Сіз бұл процесті мезгіл-мезгіл қайталай аласыз.



Интернетке қатынасу мүмкіндігі бар Басқару сервері мен оқшауланған Басқару серверлері арасында патчтар мен қажетті жаңартулар тізімін беру процесі

Интернет желісінен оқшауланған әрбір Басқару сервері (бұдан әрі – оқшауланған Басқару сервері) осы Басқару серверіне қосылған басқарылатын құрылғыларға орнатылуы қажет жаңартулар тізімін қалыптастырады. Қажетті жаңартулардың тізімі арнайы қалтада сақталады және екілік файлдар жиынтығы болып табылады. Әрбір файлда қажетті жаңарту қамтылған патч идентификаторы келтірілген атау бар. Нәтижесінде, тізімдегі әрбір файл белгілі бір патчты көрсетеді.

Сыртқы құрылғының көмегімен сіз қажетті жаңартулар тізімін оқшауланған Басқару серверінен интернетке қатынасу мүмкіндігі бар бөлектелген Басқару серверіне көшіресіз. Осыдан кейін, бөлектелген Басқару сервері интернеттен патчтарды жүктейді және оларды бөлек қалтаға салады.

Барлық патчтар жүктеліп, өздеріне арналған арнайы қалтаға орналастырылған кезде, сіз патчтарды қажетті жаңартулар тізімін алған әрбір оқшауланған Басқару серверіне жылжытасыз. Сіз патчтарды өздеріне арналған арнайы қалтаға оқшауланған Басқару серверінде сақтайсыз. Нәтижесінде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы патчтарды іске қосады және оқшауланған Басқару серверлерінің басқарылатын құрылғыларына жаңартуларды орнатады.

Оқшауланған желідегі осалдықтарды түзету үшін интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау

Оқшауланған желіде осалдықтарды түзетуге және патчтарды беруге дайындалу үшін алдымен интернетке қатынасу арқылы Басқару серверін конфигурациялаңыз, содан кейін оқшауланған Басқару серверлерін конфигурациялаңыз.

Интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау үшін:

1. Басқару сервері орнатылған дискіде екі қалта жасаңыз:

   - қажетті жаңартулар тізіміне арналған қалта;
   - патчтарға арналған қалта.

   Қалталардың атауы әртүрлі болуы мүмкін.

2. KL Admins тобына операциялық жүйені басқарудың стандартты құралдарын пайдалана отырып, жасалған қалталарды "Өзгерту" құқығын беріңіз.

3. klscflag утилитасын пайдаланып, Басқару сервері сипаттарындағы қалтаға апаратын жолдарды көрсетіңіз.

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Windows пәрмен жолына келесі пәрмендерді енгізіңіз:

   - Түзетулерге арналған қалта жолын көрсету үшін:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<қалта жолы>"`
   - Қажетті жаңартулар тізімі үшін қалта жолын белгілеу үшін:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<қалта жолы>"`

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<folder for patches>"`

5. Қажет болса, klscflag утилитасын пайдаланып, Басқару сервері жаңа түзету сұрауларын қаншалықты жиі тексеруі керек екенін көрсетіңіз:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <секундтардағы мән>`

   Әдепкі бойынша, 120 секунд мәні көрсетілген.

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларының патчтары туралы ақпаратты алу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасаңыз және тапсырманы орындау кестесін конфигурациялаңыз.

7. Осалдықтарды түзету мақсатымен пайдаланылатын үшінші тарап бағдарламаларына арналған патчтарды көрсету үшін *Осалдықтарды түзету* тапсырмасын жасаңыз және тапсырмалар кестесін конфигурациялаңыз.

   Тапсырма кестесінде көрсетілгеннен ертерек орындалуын қаласаңыз, тапсырмаларды қолмен іске қосыңыз. Тапсырмаларды іске қосу реті маңызды. *Осалдықтарды түзету* тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылуы керек.

8. Басқару сервері қызметін қайта іске қосыңыз.

Енді интернетке қатынасу мүмкіндігі бар Басқару сервері жаңартуларды жүктеуге және оқшауланған Басқару серверлеріне жіберуге дайын. Осалдықтарды түзетуді бастамас бұрын, оқшауланған Басқару серверлерін конфигурациялаңыз.

Оқшауланған желідегі осалдықтарды түзету үшін оқшауланған Басқару серверлерін конфигурациялау

Интернетке қатынасу мүмкіндігі бар Басқару серверін конфигурациялау аяқталғаннан кейін, оқшауланған Басқару серверлеріне қосылған басқарылатын құрылғыларда осалдықтарды түзете алуыңыз және жаңартуларды орната алуыңыз үшін желіңіздегі әрбір оқшауланған Басқару серверін дайындаңыз.

Оқшауланған Басқару серверлерін конфигурациялау үшін, олардың әрқайсысында келесі әрекеттерді орындаңыз:

1. Осалдықтар мен патчтарды басқару үшін лицензиялық кілтті белсендіріңіз.

2. Басқару сервері орнатылған дискіде екі қалта жасаңыз:

   - қажетті жаңартулар тізімі пайда болатын қалтаға;
   - патчтарға арналған қалта.

   Қалталардың атауы әртүрлі болуы мүмкін.

3. Операциялық жүйенің стандартты басқару құралдарын қолданып, жасалған қалталардағы KLAdmins тобына *Өзгерту* құқығын беріңіз.

4. klscflag утилитасын пайдаланып, Басқару сервері сипаттарындағы қалтаға апаратын жолдарды көрсетіңіз.

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Windows пәрмен жолына келесі пәрмендерді енгізіңіз:

   - Түзетулерге арналған қалта жолын көрсету үшін:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<қалта жолы>"`
   - Қажетті жаңартулар тізімі үшін қалта жолын белгілеу үшін:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<қалта жолы>"`

   Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<folder for patches>"`

6. Қажет болса, klscflag утилитасын пайдаланып, қашықтағы Басқару сервері жаңа патчтарды қаншалықты жиі тексеруі керек екенін көрсетіңіз:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <секундтардағы мән>
```

Әдепкі бойынша, 120 секунд мәні көрсетілген.

Мысалы: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. Қажет болса, патчтардың SHA256 хэштерін есептеу үшін klscflag утилитасын пайдаланыңыз:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```
   Осы пәрменді енгізу арқылы сіз патчтарды оқшауланған Басқару серверіне ауыстырған кезде өзгертілмегеніне және қажетті жаңартуларды қамтитын дұрыс патчтарды алғаныңызға көз жеткізе аласыз.

   Әдепкі бойынша, Kaspersky Security Center қолданбасы SHA-256 патч хэштерін есептемейді. Егер сіз осы параметрді қоссаңыз, патчтарды оқшауланған Басқару сервері алғаннан кейін, Kaspersky Security Center бағдарламасы олардың хэштерін есептейді және алынған мәндерді Басқару серверінің дерекқорында сақталған хэштермен салыстырады. Егер есептелген хэш дерекқордағы хэшке сәйкес келмесе, қате пайда болып, дұрыс емес патчтарды ауыстыру қажет болады.

8. Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларының патчтары туралы ақпаратты алу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасаңыз және тапсырманы орындау кестесін конфигурациялаңыз.

9. Осалдықтарды түзету мақсатымен пайдаланылатын үшінші тарап бағдарламаларына арналған патчтарды көрсету үшін *Осалдықтарды түзету* тапсырмасын жасаңыз және тапсырмалар кестесін конфигурациялаңыз.

   Тапсырма кестесінде көрсетілгеннен ертерек орындалуын қаласаңыз, тапсырмаларды қолмен іске қосыңыз. Тапсырмаларды іске қосу реті маңызды. *Осалдықтарды түзету* тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылуы керек.

10. Басқару сервері қызметін қайта іске қосыңыз.

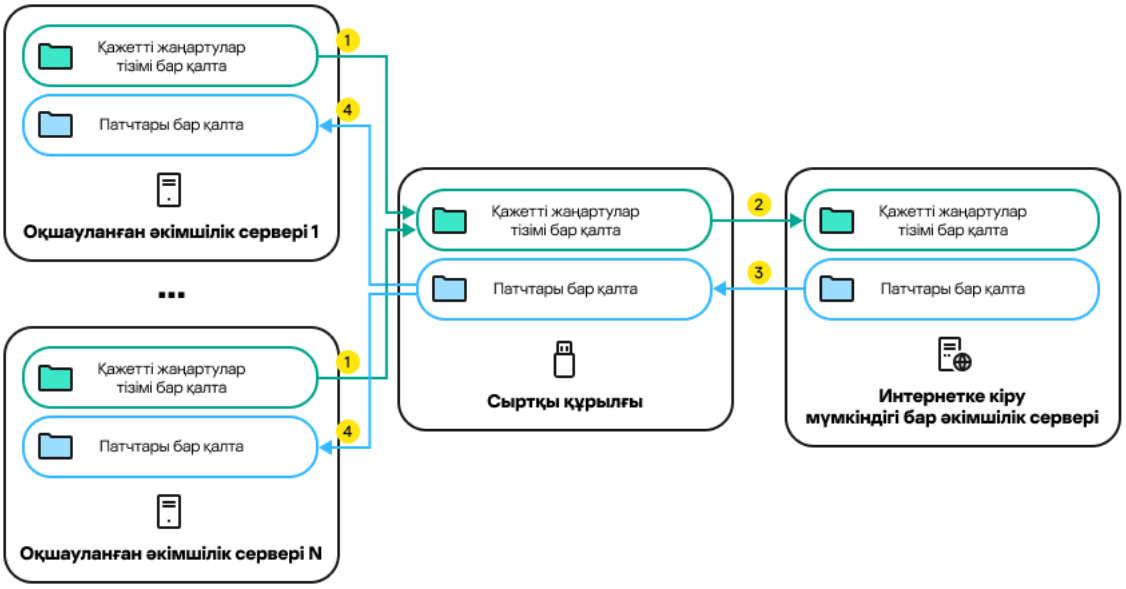
Барлық Басқару серверлерін орнатқаннан кейін, сіз түзетулер мен қажетті жаңартулар тізімдерін жылжыта аласыз және оқшауланған желідегі басқарылатын құрылғылардағы үшінші тарап бағдарламаларының осалдықтарын түзете аласыз.

Оқшауланған желіде түзетулерді беру және жаңартуларды орнату

Басқару серверлерін конфигурациялау аяқталғаннан кейін, сіз патчтарды қажетті жаңартулармен бірге интернетке қатынасу мүмкіндігі бар Басқару серверінен оқшауланған Басқару серверлеріне ауыстыра аласыз. Жаңартуларды қажет жиілікпен, мысалы күніне бір немесе бірнеше рет беруге және орнатуға болады.

Сыртқы диск сияқты алынбалы диск Басқару серверлері арасында патчтарды және қажетті жаңартулар тізімін тасымалдау үшін қажет. Сыртқы дискіде патчтарды жүктеу және сақтау үшін жеткілікті орын бар екеніне көз жеткізіңіз.

Патчтар мен қажетті жаңартулар тізімін беру процесі суретте көрсетілген және төменде сипатталған:



Интернетке қатынасу мүмкіндігі бар Басқару сервері мен оқшауланған Басқару серверлері арасында патчтар мен қажетті жаңартулар тізімін беру процесі

Оқшауланған Басқару серверлеріне қосылған басқарылатын құрылғыларда жаңартуларды орнату және осалдықтарды түзету үшін:

1. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы әлі іске қосылмаса, оны іске қосыңыз.

2. Сыртқы дискіні кез келген оқшауланған Басқару серверіне қосыңыз.

3. Сыртқы дискіде екі қалта жасаңыз: біреуі – қажетті жаңартулар тізіміне, екіншісі – патчтарға арналған. Қалталардың атауы әртүрлі болуы мүмкін.

   Егер сіз бұл қалталарды бұрын жасаған болсаңыз, оларды тазалаңыз.

4. Әрбір оқшауланған Басқару серверінен қажетті жаңартулар тізімін көшіріп, осы тізімді сыртқы дискідегі қажетті жаңартулар тізіміне арналған қалтаға салыңыз.

   Нәтижесінде, сіз барлық оқшауланған Басқару серверлерінен алынған барлық тізімдерді бір қалтаға біріктіресіз. Бұл қалтада барлық оқшауланған Басқару серверлеріне қажет патч идентификаторлары бар екілік файлдар болуы керек.

5. Сыртқы дискіні интернетке қатынасу мүмкіндігі бар Басқару серверіне қосыңыз.

6. Қажетті жаңартулар тізімін сыртқы дискіден көшіріп, осы тізімді интернетке қатынасу мүмкіндігі бар Басқару серверіндегі қажетті жаңартулар тізіміне арналған қалтаға салыңыз.

   Барлық қажетті патчтар автоматты түрде интернеттен Басқару серверіндегі патчтар қалтасына жүктеледі. Бұған бірнеше сағат кетуі мүмкін.

7. Барлық қажетті патчтардың жүктелгеніне көз жеткізіңіз. Ол үшін келесі әрекеттердің бірін орындауға болады:

   - Интернетке қатынасу мүмкіндігі бар Басқару серверіндегі патчтар үшін қалтаны тексеріңіз. Қажетті жаңартулар тізімінде көрсетілген барлық түзетулер қажетті қалтаға жүктелуі керек. Егер аздаған түзету қажет болса, бұл ыңғайлырақ.

   - Shell-скрипт сияқты арнайы скриптті дайындаңыз. Егер сіз көп патч алсаңыз, онда барлық түзетулердің жүктелгенін өзіңізге тексеру қиын болады. Мұндай жағдайларда, тексеруді автоматтандырған дұрыс.

8. Патчтарды интернетке қатынасу мүмкіндігі Басқару серверінен көшіріп, сыртқы дискідегі тиісті қалтаға салыңыз.

9. Патчтарды әр оқшауланған Басқару серверіне тасымалдаңыз. Патчтарды өздеріне арналған арнайы қалтаға салыңыз.

Нәтижесінде, әрбір оқшауланған Басқару сервері ағымдағы Басқару серверіне қосылған басқарылатын құрылғылар үшін қажетті жаңартулардың ағымдағы тізімін жасайды. Қажетті жаңартулардың тізімін алғаннан кейін Басқару сервері интернеттен патчтарды жүктейді. Осы патчтар оқшауланған Басқару серверлерінде пайда болған кезде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы патчтарды өңдейді. Осылайша, басқарылатын құрылғыларға жаңартулар орнатылады және үшінші тарап бағдарламаларындағы осалдықтар түзетіледі.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын орындаған кезде Басқару серверінің құрылғысына артық жүктеме түсірмеңіз және *Басқару сервері деректерінің резервтік қоймасы* тапсырмасын іске қоспаңыз (бұл да артық жүктелуге себеп болады). Нәтижесінде, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы үзіледі, ал жаңартулар орнатылмайды. Бұл жағдайда, сіз бұл тапсырманы қолмен қайта бастауыңыз немесе тапсырманың конфигурацияланған кесте бойынша басталуын күтуіңіз керек.

Оқшауланған желіде түзетулерді жіберу және жаңартуларды орнату мүмкіндігін өшіру

Оқшауланған Басқару серверлеріне түзетулерді жіберуді өшіруге болады, мысалы, егер сіз оқшауланған желіден бір немесе бірнеше Басқару серверін шығаруды шешсеңіз. Осылайша, сіз түзетулер санын және оларды жүктеу уақытын қысқарта аласыз.

Патчтарды оқшауланған Басқару серверлеріне беру мүмкіндігін өшіру үшін:

1. Егер сіз барлық Басқару серверлерін оқшаулаудан шығарғыңыз келсе, интернетке қатынасу мүмкіндігі бар Басқару серверінің сипаттарында патч қалталарына апаратын жолдарды және қажетті жаңартулар тізімін жойыңыз. Егер сіз кейбір Басқару серверлерінің оқшауланған желіде болуын қаласаңыз, бұл қадамды өткізіп жіберіңіз.

   Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Пәрмен жолына келесі пәрмендерді енгізіңіз:

   - Патч қалтасына апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

   - Қажетті жаңартулар тізімі бар қалтаға апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Егер сіз осы Басқару серверіндегі қалталарға апаратын жолдарды жойсаңыз, Басқару сервері қызметін қайта іске қосыңыз.

3. Оқшауланғыңыз келетін әрбір Басқару серверінің сипаттарында патч қалталарына апаратын жолдарды және қажетті жаңартулар тізімін жойыңыз.

   Windows пәрмен жолында келесі пәрмендерді әкімші құқықтарымен енгізіңіз:

   - Патч қалтасына апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - Қажетті жаңартулар тізімі бар қалтаға апаратын жолды жою үшін:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Қалталарға апаратын жолдар жойылған әрбір Басқару сервері қызметін қайта іске қосыңыз.

Егер сіз интернетке қатынасу мүмкіндігі бар Басқару серверін қайта конфигурациялаған болсаңыз, сіз енді Kaspersky Security Center арқылы патчтарды алмайсыз. Егер сіз тек кейбір оқшауланған Басқару серверлерін қайта конфигурациялаған болсаңыз, мысалы, кейбіреулерін оқшауланған желіден шығару арқылы сіз тек оқшауланған Басқару серверлеріне арналған патчтарды аласыз.

Егер сіз болашақта ажыратылған оқшауланған Басқару серверлеріндегі осалдықтарды түзетуді бастағыңыз келсе, онда сіз осы Басқару серверлері мен интернетке қатынасу мүмкіндігі бар Басқару серверін тағы бір рет конфигурациялауыңыз керек.

Бағдарламалардағы осалдықтарды елемеу

Бағдарламалық жасақтама осалдықтарын елемеуіңіз және оларды түзетпеуіңіз мүмкін. Бағдарламалардағы осалдықтарды елемеу себептері, мысалы, келесідей болуы мүмкін:

- Сіз бағдарламадағы осалдықты ұйымыңыз үшін критикалық деп санамайсыз.
- Бағдарламалық жасақтама осалдықтарын түзету, осалдықты түзетуді қажет ететін бағдарламаның деректерін зақымдауы мүмкін екенін түсінесіз.
- Бағдарламалық жасақтама осалдықтары сіздің ұйымыңыздың желісіне қауіп төндірмейтініне сенімдісіз, өйткені сіз басқарылатын құрылғыларды қорғау үшін басқа шараларды қолданасыз.

Барлық басқарылатын құрылғылардағы немесе тек таңдалған басқарылатын құрылғылардағы бағдарламалардағы осалдықты елемеуге болады.

Барлық басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын өткізіп жіберу үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама осалдықтары** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында, оларға орнатылған Желілік агент анықтаған құрылғылардағы бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

2. Өткізіп жібергіңіз келетін осалдықты таңдаңыз.

3. Осалдықтың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   Осалдық сипаттары терезесі ашылады.

4. **Жалпы** бөлімінде **Осалдықты елемеу** параметрін таңдаңыз.

5. **OK** түймесін басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттарының терезесі жабылады.

Бағдарламалық жасақтама осалдықтары барлық басқарылатын құрылғыларда өткізіп жіберіледі.

Таңдалған басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын өткізіп жіберу үшін:

1. Таңдалған басқарылатын құрылғы сипаттары терезесін ашып, **Бағдарламалық жасақтама осалдықтары** бөлімін таңдаңыз.

2. Бағдарламалық жасақтама осалдықтарын таңдаңыз.

3. Таңдалған осалдықты өткізіп жіберіңіз.

Бағдарламалық жасақтама осалдықтары таңдалған құрылғыда өткізіп жіберіледі.

Өткізіп жіберілген бағдарламалық жасақтама осалдықтары *Осалдықтарды түзету* және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмаларының жұмысы аяқталғаннан кейін жабылмайды. Бағдарламалардағы жетіспейтін осалдықтарды осалдықтар тізімінен сүзгі арқылы алып тастауға болады.

Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушы түзетулері

Осалдықтарды түзету тапсырмасын пайдалану үшін, тапсырма параметрлерінде тізімделген үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін бағдарламалық жасақтама жаңартуларын қолмен көрсету керек. *Осалдықтарды түзету* тапсырмасы Microsoft бағдарламаларының ұсынылған түзетулерін және басқа үшінші тарап бағдарламалары үшін пайдаланушылық түзетулерді пайдаланады. *Пайдаланушылық түзетулер* – бұл әкімші орнату үшін қолмен көрсететін осалдықтарды түзетуге арналған бағдарламалық жасақтама жаңартулары.

Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушылық түзетулерді таңдау үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалық жасақтама осалдықтары** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында, оларға орнатылған Желілік агент анықтаған құрылғылардағы бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

2. Пайдаланушылық түзетуді көрсеткіңіз келетін осалдықты таңдаңыз.

3. Осалдықтың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   Осалдық сипаттары терезесі ашылады.

4. **Пайдаланушылық және басқа түзетулер** бөлімінде **Қосылуда** түймесін басыңыз.

   Қолжетімді орнату пакеттері тізімі көрсетіледі. Пайда болған орнату пакеттері тізімі **Қашықтан орнату** → **Орнату пакеттері** қалтасындағы тізімге сай келеді. Егер сіз таңдалған осалдықты түзету үшін пайдаланушылық түзетуді қамтитын орнату пакетін жасамаған болсаңыз, орнату пакетін жасау шеберін іске қосу арқылы пакетті қазір жасауға болады.

5. Үшінші тарап бағдарламаларының осалдығы үшін пайдаланушылық түзетуді (немесе пайдаланушылық түзетулерді) қамтитын орнату пакетін (немесе пакеттерін) таңдаңыз.

6. **OK** түймесін басыңыз.

Бағдарламалық жасақтама осалдықтарына арналған пайдаланушылық түзетулерді қамтитын орнату пакеттері көрсетілген. *Осалдықтарды түзету* тапсырмасын іске қосқаннан кейін, орнату пакеті орнатылып, бағдарламалық жасақтама осалдықтары жабылады.

Жаңартулар орнату ережелері

Бағдарламалық жасақтама осалдықтарын түзету үшін жаңартулар орнату ережелерін көрсету керек. Бұл ережелер орнатылатын жаңартуларды және түзетілетін осалдықтарды анықтайды.

Нақты параметрлер, Microsoft бағдарламаларын, үшінші тарап бағдарламаларын (Kaspersky мен Microsoft корпорациясынан басқа бағдарламалық жасақтама жеткізушілері шығаратын бағдарламалар) немесе барлық бағдарламаларды жаңарту ережесін құрғаныңызға байланысты болады. Microsoft бағдарламалары немесе үшінші тарап бағдарламалары үшін ереже жасағанда, жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдауға болады. Барлық бағдарламалар үшін ереже жасағанда, сіз орнатылатын жаңартуларды және жаңартуларды орнату арқылы түзетілетін осалдықтарды таңдай аласыз.

Бағдарламаларды жаңарту ережесін жасау үшін:

1. Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

2. **Ереже түрі** бетінде **Барлық жаңартуларға арналған ереже** таңдаңыз.

3. Ашылмалы тізімдегі **Жалпы критерийлер** терезесінде келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Жаңартулар** терезесінде орнатылатын жаңартуларды таңдаңыз:

   - **Барлық жарамды жаңартуларды орнату**

     Бұл жағдайда, **Жалпы критерийлер** шебері терезесінде көрсетілген өлшемшарттарға сәйкес келетін бағдарламалық жасақтаманың барлық жаңартулары орнатылады. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі жаңартуларды орнату**

     Бұл жағдайда, тізімде қолмен таңдайтын бағдарламалық жасақтаманың жаңартулары ғана орнатылады. Бұл тізімде барлық қолжетімді бағдарламалық жасақтама жаңартулары бар.

     Мысалы, келесі жағдайларда жаңартуларды орнатуға болады: тек критикалық маңызды бағдарламаларды жаңарту үшін немесе тек қажетті бағдарламаларды жаңарту үшін сынақ ортасында жаңартуларды орнатуды тексеру.

     - **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

       Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

       Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

       Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

       Әдепкі бойынша, параметр қосулы.

5. **Осалдықтар** терезесінде, көрсетілген жаңартуды орнатумен түзетілетін осалдықтарды таңдаңыз:

   - **Қалған критерийлерге сай барлық осалдықтарды жабу**

     Бұл жағдайда, **Жалпы критерийлер** шебері терезесінде көрсетілген өлшемшарттарға сәйкес келетін бағдарламалық жасақтаманың барлық осалдықтары түзетіледі. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі осалдықтарды жабу**

     Тізімнен қолмен таңдалған осалдықтарды ғана түзетіңіз. Бұл тізімде барлық анықталған осалдықтар бар.

     Мысалы, келесі жағдайларда осалдықтарды белгілеуге болады: сынақ ортасындағы осалдықтардың түзетілуін тексеру, тек маңызды бағдарламалардағы осалдықтарды түзету немесе тек қажетті бағдарламалардағы осалдықтарды түзету үшін.

6. **Атауы** терезесінде жасалатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ережені жасау шебері өз жұмысын аяқтағаннан кейін, ереже жасалады және жаңа тапсырма жасау шеберінің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** өрісінде көрсетіледі.

Microsoft бағдарламаларын жаңарту ережесін жасау үшін:

1. Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

2. **Ереже түрі** бетінде **Windows Update жаңартуларына арналған ереже** таңдаңыз.

3. **Жалпы критерийлер** бетінде келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

   - **MSRC бойынша қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Жаңартулардың санаттары** терезесінде орнату үшін жаңарту санаттарын таңдаңыз. Бұл санаттар Microsoft Update каталогымен бірдей. Әдепкі бойынша барлық санаттар таңдалған.

6. **Атауы** терезесінде жасалатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ережені жасау шебері өз жұмысын аяқтағаннан кейін, ереже жасалады және жаңа тапсырма жасау шеберінің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** өрісінде көрсетіледі.

Үшінші тарап бағдарламаларын жаңарту ережесін жасау үшін:

1. Жаңа тапсырма жасау шеберінің **Параметрлер** терезесінде **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

2. **Ереже түрі** бетінде **Үшінші тарап жаңартуларға арналған ереже** таңдаңыз.

3. **Жалпы критерийлер** бетінде келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Атауы** терезесінде жасалатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ережені жасау шебері өз жұмысын аяқтағаннан кейін, ереже жасалады және жаңа тапсырма жасау шеберінің **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз** өрісінде көрсетіледі.

Бағдарламалар топтары

Бұл бөлімде құрылғыларда орнатылған бағдарламалар топтарымен жұмыс сипатталған.

Бағдарлама санаттарын жасау

Kaspersky Security Center құрылғыларда орнатылған бағдарламалардың санаттарын жасауға мүмкіндік береді.

Бағдарлама санаттарын келесі тәсілдермен жасауға болады:

- Әкімші орындалатын файлдар таңдалған санатқа кіретін қалтаны көрсетеді.
- Әкімші орындалатын файлдар таңдалған санатқа жататын құрылғыны көрсетеді.
- Әкімші бағдарламалардың таңдалған санатқа ену критерийлерін белгілейді.

Бағдарламалар санаты құрылған кезде әкімші бағдарламалардың осы санаты үшін ережелерді белгілей алады. Ережелер көрсетілген санатқа кіретін бағдарламалардың әрекетін анықтайды. Мысалы, санатқа кіретін бағдарламалардың іске қосылуына тыйым салуға немесе рұқсат беруге болады.

Құрылғыларда бағдарламалардың іске қосылуын басқару

Kaspersky Security Center бағдарламасы "Рұқсат ету тізімі" режимінде құрылғыларда бағдарламалардың іске қосылуын басқаруға мүмкіндік береді. Толық сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген. Таңдалған құрылғыларда "Рұқсат ету тізімі" режимінде тек көрсетілген санаттарға кіретін бағдарламаларды іске қосуға рұқсат етіледі. Әкімші әр пайдаланушы үшін құрылғылардағы бағдарламаларды іске қосу ережелерін статикалық талдау нәтижелерін көре алады.

Құрылғыларда орнатылған бағдарламалық жасақтаманы түгендеу

Kaspersky Security Center қызметі Windows және Linux басқаратын құрылғыларда бағдарламалық жасақтаманы түгендеуге мүмкіндік береді. Желілік агент құрылғыларға орнатылған барлық бағдарламалар туралы ақпарат алады. Түгендеу нәтижесінде алынған ақпарат **Бағдарламалар тізімдемесі** қалтасының жұмыс аймағында көрсетіледі. Әкімші әр бағдарлама туралы егжей-тегжейлі ақпаратты, соның ішінде нұсқасы мен өндірушісін көре алады.

Бір құрылғыдан алынатын орындалатын файлдар саны 150 000-нан аса алмайды. Осы шектеуге жеткеннен кейін, Kaspersky Security Center жаңа файлдарды алмайды.

Лицензиялы бағдарламалар топтарын басқару

Kaspersky Security Center лицензиялы бағдарламалар топтарын құруға мүмкіндік береді. Лицензиялы бағдарламалар тобына әкімші белгілеген критерийлерге сәйкес келетін бағдарламалар кіреді. Әкімші лицензиялы бағдарламалар топтары үшін келесі критерийлерді көрсете алады:

- Бағдарлама атауы
- Бағдарлама нұсқасы
- Өндіруші
- Бағдарлама тегі

Бір немесе бірнеше критерийге сәйкес келетін бағдарламалар автоматты түрде топқа енеді. Лицензиялы бағдарламалар тобын құру үшін осы топқа бағдарламаларды қосудың кем дегенде бір критерийі көрсетілуі керек.

Лицензиялы бағдарламалардың әр тобында өзінің лицензиялық кілті бар. Лицензиялық бағдарламалар тобының лицензиялық кілті топқа кіретін бағдарламалар үшін орнатудың рұқсат етілген санын анықтайды. Егер орнату саны лицензиялық кілтте көрсетілген шектен асып кетсе, Басқару серверінде ақпараттық оқиға тіркеледі. Әкімші лицензиялық кілттің аяқталу күнін көрсете алады. Осы күн келгенде Басқару серверінде ақпараттық оқиға тіркеледі.

Орындалатын файлдар туралы ақпаратты қарау

Kaspersky Security Center құрылғыларда операциялық жүйе орнатылған сәттен бастап іске қосылған орындалатын файлдар туралы барлық ақпаратты алады. Орындалатын файлдар туралы алынған ақпарат **Орындалатын файлдар** қалтасының жұмыс аймағындағы Бағдарламаның негізгі терезесінде көрсетіледі.

Орындалатын файлдарды басқару үшін Бағдарламаларды басқару компонентін пайдалану

Пайдаланушы құрылғыларында орындалатын файлдардың орындалуына рұқсат беру немесе тыйым салу үшін Бағдарламаларды бақылау компонентін пайдалануға болады. Бағдарламаларды бақылау компоненті Windows және Linux операциялық жүйелерін қолдайды.

Linux негізіндегі операциялық жүйелер үшін қолданбаларды басқару құрамдасы Linux-ке арналған Kaspersky Endpoint Security 11.2 нұсқасынан бастап қолжетімді. Сондай-ақ құрамдас Windows 3.0 немесе одан кейінгі нұсқасына арналған Kaspersky Embedded Systems Security үшін қолжетімді.

Алдын ала талаптар

- Kaspersky Security Center бағдарламасы сіздің ұйымыңызда орналастырылған.
- Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Linux саясаты жасалды және белсенді.
- Kaspersky Embedded Systems Security for Windows немесе Kaspersky Embedded Systems Security for Linux саясаты жасалды және белсенді.

Кезеңдер

Бағдарламаны басқару құрамдасын қолдану сценарийі келесі кезеңдерден тұрады:

1. **Клиент құрылғыларында орындалатын файлдар тізімін құрастыру және қарау**

Бұл кезең сізге басқарылатын құрылғыларда қандай орындалатын файлдардың орнатылғанын анықтауға көмектеседі. Орындалатын файлдар тізімін қарап шығыңыз және оны рұқсат етілген және тыйым салынған орындалатын файлдардың тізімдерімен салыстырыңыз. Орындалатын файлдарды қолданудағы шектеулер ұйымдағы ақпараттық қауіпсіздік саясаттарымен байланысты болуы мүмкін.

Нұсқаулар:

- Басқару консолі: Орындалатын файлдарды түгендеу.
- Kaspersky Security Center Web Console: Клиент құрылғыларында сақталатын орындалатын файлдар тізімін алу және қарау.

2. **Ұйымыңызда қолданылатын орындалатын файлдар үшін санаттарды жасау**

Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімдерін талдаңыз. Талдау негізінде орындалатын файлдар үшін санаттарды қалыптастырыңыз. Ұйымыңызда қолданылатын орындалатын файлдардың стандартты жиынтығын қамтитын "Жұмыс бағдарламалары" санатын құру ұсынылады. Егер әртүрлі қауіпсіздік топтары өз жұмысында өзіндік орындалатын файлдар жиынтығын қолданса, әр қауіпсіздік тобы үшін бөлек санатты құруға болады.

Нұсқаулар:

- Басқару консолі: Қолмен толықтырылатын бағдарламалар санатын құру, Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын құру, Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру.
- Kaspersky Security Center Web Console: Қолмен толықтырылатын бағдарламалар санатын құру, Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын құру, Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру.

3. **Kaspersky Endpoint Security саясатындағы Бағдарламаларды басқару конфигурациялау**

Алдыңғы кезеңде жасаған санаттарды қолдана отырып, Kaspersky Endpoint Security саясатындағы Бағдарламаларды басқару құрамдасын конфигурациялаңыз.

Нұсқаулар:

- Басқару консолі: Клиент құрылғыларында бағдарламаларды іске қосуды басқаруды конфигурациялау.
- Kaspersky Security Center Web Console: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау.

4. **Kaspersky Embedded Systems Security қолданба саясатындағы қолданбаларды басқаруды конфигурациялау**

Жасалған санаттарды пайдалану арқылы Kaspersky Embedded Systems Security for Windows саясатындағы қолданбаларды басқару құрамдасын конфигурациялаңыз. Қолданбаларды басқару құрамдасы туралы қосымша ақпарат алу үшін Kaspersky Embedded Systems Security for Windows Help немесе Kaspersky Embedded Systems Security for Linux анықтамасын қараңыз.

Ережелердің көп санын пайдалансаңыз, саясатты жүктеу кезінде қате орын алуы мүмкін. Келесі пәрмендерді пайдалану байт өлшеміндегі максималды сұрау өлшемін арттыруға болады:

- JSON сұрауы үшін:

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
```

- HTTP сұрауы үшін:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Бұл жерде `<max_request_size>` — байт өлшеміндегі максималды сұрау өлшемі (мысалы, `200000000`).

5. **Тест режимінде Бағдарламаларды басқару құрамдасын қосу**

   Бағдарламаларды басқару ережелері пайдаланушылардың жұмысына қажетті орындалатын файлдарды бұғаттамауы үшін, Қолданбаларды бақылау ережелерін тестілеуді қосып, ережелер жасалғаннан кейін олардың жұмысын талдау ұсынылады. Сынау қосылған кезде, Kaspersky Endpoint Security for Windows немесе Kaspersky Embedded Systems Security саясаты қолданбаларды басқару ережелері іске қосуды тыйым салынған орындалатын файлдарды бұғаттамайды, бірақ оның орнына басқару серверіне олардың іске қосылуы туралы хабарландырулар жібереді.

   Бағдарламаларды бақылау ережелерін тестілеу кезінде келесі әрекеттерді орындау ұсынылады:

   - Тестілеу кезеңін анықтаңыз. Тестілеу кезеңі бірнеше күннен екі айға дейін өзгеруі мүмкін.
   - Бағдарламаны басқару құрамдасының жұмысын тексеру нәтижесінде пайда болатын оқиғаларды зерттеңіз.

   Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындаңыз және орнату процесінде **Сынақ режимі** опциясын қосыңыз.

6. **Бағдарламаны басқару құрамдасының санаттары параметрлерін өзгерту**

   Қажет болса, Бағдарламаларды басқару құрамдасының параметрлерін өзгертіңіз. Тестілеу нәтижелеріне сүйене отырып, Бағдарламаларды басқару құрамдасының оқиғаларына байланысты орындалатын файлдарды қолмен толықтырылатын санатқа қосуға болады.

   Нұсқаулар:

   - Басқару консолі: Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу.
   - Kaspersky Security Center Web Console: Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу.

7. **Жұмыс режимінде Бағдарламаларды бақылау ережелерін қолдану**

   Бағдарламаларды бақылау ережелерін тексергеннен кейін және санаттарды конфигурациялауды аяқтағаннан кейін, сіз жұмыс режимінде Бағдарламаларды басқару ережелерін қолдана аласыз.

   Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындап, конфигурациялау барысында **Сынақ режимі** параметрін өшіріңіз.

8. **Бағдарламаны басқару конфигурациясын тексеру**

   Келесіні орындағаныңызға көз жеткізіңіз:

   - Орындалатын файлдар үшін санаттар жасадық.
   - Санаттарды қолдана отырып, Бағдарлама санаттарын конфигурацияладыңыз.
   - Жұмыс режимінде Бағдарламаларды бақылау ережелерін қолдандыңыз.

Нәтижелер

Сценарий аяқталғаннан кейін, басқарылатын құрылғыларда орындалатын файлдардың іске қосылуы бақыланады. Пайдаланушылар сіздің ұйымыңызда рұқсат етілген орындалатын файлдарды ғана басқара алады және сіздің ұйымыңызда тыйым салынған орындалатын файлдарды іске қоса алмайды.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау

Клиент құрылғыларында сақталған орындалатын файлдар тізімін келесі жолдардың бірімен алуға болады:

- Kaspersky Endpoint Security саясатында қолданбаларды іске қосу туралы хабарландыруларды қосу.
- Түгендеу тапсырмасын жасау.

Kaspersky Endpoint Security саясатында қолданбаларды іске қосу туралы хабарландыруларды қосу

Бағдарламаларды іске қосу туралы хабарландыруларды қосу үшін:

1. Kaspersky Endpoint Security саясат параметрлерін ашыңыз, содан кейін **Жалпы параметрлер** → **Есептер және қоймалар** тармағына өтіңіз.
2. **Деректерді әкімші серверіне тасымалдау** параметрлер тобында **Іске қосылған қолданбалар туралы ақпарат** құсбелгісін қойып, өзгерістерді сақтаңыз.

Пайдаланушы орындалатын файлдарды іске қосуға әрекет жасағанда, осы файлдар туралы ақпарат клиент құрылғысындағы орындалатын файлдар тізіміне қосылады. Kaspersky Endpoint Security бұл ақпаратты желілік агентке жібереді, содан кейін желілік агент оны басқару серверіне жібереді.

Түгендеу тапсырмасын жасау

Орындалатын файлдарды түгендеу функциясы келесі бағдарламалар үшін қолжетімді:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 11.2 және одан жоғары нұсқалары
- Kaspersky Security for Virtualization 4.0 Light Agent және одан да жоғары

Орнатылған бағдарламалар туралы ақпаратты алу арқылы дерекқорға түсетін жүктемені азайтуға болады. Бос орын үнемдеу үшін бағдарламалық жасақтаманың стандартты жинағы сақталған анықтамалық құрылғыларда түгендеу тапсырмасын іске қосыңыз. Құрылғылардың саны 1-3 болғаны дұрыс.

Төмендегі дерекқорларды пайдаланған кезде түгендеу тапсырмасын орындамаған жөн: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (барлық шығарылым).

Клиент құрылғыларында орындалатын файлдарды түгендеу тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Тапсырмалар** қалтасының жұмыс аймағындағы **Жаңа тапсырма** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрін таңдау** шебері терезесінде **Kaspersky Endpoint Security** тапсырма түрін, содан соң **Түгендеу** тапсырмасы ішкі түрін таңдап, **Келесі** түймесін басыңыз.
4. Шебердің келесі қадамдарын орындаңыз.

   Жаңа тапсырма жасау шебері өз жұмысын аяқтағаннан кейін, **Қойма** тапсырмасы жасалды және конфигурацияланды. Сіз жасалған тапсырманың параметрлерін өзгерте аласыз. Нәтижесінде, жасалған тапсырма тапсырмалар тізімінде көрсетіледі. Сіз жасалған тапсырманың параметрлерін өзгерте аласыз.

Түгендеу тапсырмасының толық сипаттамасын келесі анықтамалардан қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент

Қойма тапсырмасын орындағаннан кейін, басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімі жасалады және сіз осы тізімді қарай аласыз.

Түгендеу кезінде келесі форматтағы орындалатын файлдарды анықтауға болады (түгендеу тапсырмасы сипаттарында таңдалған опцияға байланысты): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімін көру.

Клиент құрылғыларында сақталатын орындалатын файлдар тізімін көру үшін,

Консоль тармағында **Қосымша** → **Қолданбаларды басқару** → **Орындалатын файлдар** тармағына өтіңіз.

Қажет болса, басқарылатын құрылғыдан басқару консолі орнатылған құрылғыға орындалатын файлды жіберуге болады.

Орындалатын файлды жіберу үшін:

1. Консоль тармағында **Қосымша** → **Қолданбаларды басқару** → **Орындалатын файлдар** тармағына өтіңіз.
2. Басқару консолі орнатылған құрылғыға жібергіңіз келетін орындалатын файлдың сілтемесін басыңыз.
3. Ашылған терезеде **Құрылғылар** бөліміне өтіп, орындалатын файлды жібергіңіз келетін басқарылатын құрылғының жанына жалаушаны қойыңыз.

   Орындалатын файлды жібермей тұрып, **Басқару серверімен байланысты үзбеу** құсбелгі ұяшығын таңдап, басқарылатын құрылғыда басқару серверімен тікелей байланыс бар екенін тексеріңіз.

4. **Жіберу** түймесін басып, тарату қалтасын таңдап, **OK** түймесін басыңыз.

Таңдалған орындалатын файл басқару консолі орнатылған құрылғыға одан әрі жіберу үшін жүктеп алынады.

Kaspersky Endpoint Security для Windows саясаты үшін бағдарлама санаттарын жасау

Kaspersky Endpoint Security for Windows саясатына арналған бағдарламалар санаттарын **Бағдарлама санаттары** қалтасында және Kaspersky Endpoint Security for Windows саясатының **Сипаттар** терезесінде жасауға болады.

***Бағдарлама санаттары** қалтасында Kaspersky Endpoint Security саясаты үшін бағдарламаларын санатын жасауға болады:*

1. Консоль ағашында **Кеңейтілген** → **Бағдарламаларды басқару** → **Бағдарлама санаттары** тармағын таңдаңыз.
2. **Бағдарлама санаттары** қалтасының жұмыс аймағындағы **Жаңа санат** түймесін басыңыз.

   Жаңа санат шебері іске қосылады.

3. Шебердің **Санат түрі** терезесінде пайдаланушы санаты түрін таңдаңыз:

   - **Қолмен толтырылатын санат**. Орындалатын файлдар жасалатын санатқа жататын критерийлерді белгілеңіз.
   - **Автоматты түрде толтырылатын санат**. Жасалған санатқа орындалатын файлдар автоматты түрде қосылатын қалтаны көрсетіңіз.

     Автоматты түрде толтырылатын санатты жасаған кезде қолданба келесі файл түрлерін түгендейді: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX және SCR.

   - **Таңдалған құрылғылардағы орындалатын файлдар кіретін санат**. Орындалатын файлдары автоматты түрде санатқа енуі керек құрылғыны көрсетіңіз.

4. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебер аяқталғаннан кейін, реттелмелі бағдарламалар санаттары құрылады. Жасалған санатты **Бағдарлама санаттары** қалтасының жұмыс аймағындағы санаттар тізімінде қарауға болады.

Қолданба санатын KLC файлына экспорттағыңыз келсе, санат атауын тінтуірдің оң жақ түймесімен басып, мәзірден **Экспорттау** опциясын таңдаңыз, содан кейін ашылатын терезеде файл атауын көрсетіңіз де, **Сақтау** түймесін басыңыз.

Сондай-ақ, бағдарламалар санатын **Саясаттар** қалтасында жасауға болады.

*Kaspersky Endpoint Security for Windows саясатының **Сипаттар** терезесінде бағдарламалар санатын жасау үшін:*

1. Консоль ағашында **Саясаттар** қалтасын таңдаңыз.
2. **Саясаттар** қалтасының жұмыс аймағында бағдарламалар санатын жасауды қажет ететін Kaspersky Endpoint Security саясатын таңдаңыз.
3. Мәнмәтіндік мәзірде **Сипаттар** тармағын таңдаңыз.
4. Ашылған **Сипаттар** терезесіндегі **Бөлімдер** панелінде **Қауіпсіздікті бақылау** → **Бағдарламаны басқару** бөлімін таңдаңыз.
5. **Бағдарламаны басқару** бөлімінде, **Бағдарламаны басқару режимі** және **Әрекет** ашылмалы тізімінде Тыйым салу тізімін немесе Рұқсат ету тізімін таңдап, **Қосу** түймесін басыңыз.

   Санаттар тізімін қамтитын **Бағдарламаны басқару ережесі** терезесі ашылады.

6. **Жасау** түймесін басыңыз.
7. Санат атауын енгізіп, **OK** түймесін басыңыз.

   Жаңа санат шебері іске қосылады.

8. Шебердің **Санат түрі** терезесінде пайдаланушы санаты түрін таңдаңыз:

   - **Қолмен толтырылатын санат**. Орындалатын файлдар жасалатын санатқа жататын критерийлерді белгілеңіз.
   - **Автоматты түрде толтырылатын санат**. Жасалған санатқа орындалатын файлдар автоматты түрде қосылатын қалтаны көрсетіңіз.

     Автоматты түрде толтырылатын санатты жасаған кезде қолданба келесі файл түрлерін түгендейді: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX және SCR.

   - **Таңдалған құрылғылардағы орындалатын файлдар кіретін санат**. Орындалатын файлдары автоматты түрде санатқа енуі керек құрылғыны көрсетіңіз.

9. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебер аяқталғаннан кейін, реттелмелі бағдарламалар санаттары құрылады. Жаңа санатты бағдарлама санаттары тізімінен көруге болады.

Бағдарлама санаттарын Kaspersky Endpoint Security for Windows қауіпсіздік бағдарламасының құрамына кіретін бағдарламаларды басқару құрамдасы пайдаланады. Бағдарламаны басқару құрамдасы әкімшіге клиент құрылғыларында бағдарламаларды іске қосуға шектеулер қоюға мүмкіндік береді, мысалы, таңдалған санатқа кіретін бағдарламалар негізінде.

Қолмен толықтырылатын бағдарламалар санатын жасау

Сіз өзіңіздің ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдарға арналған үлгі ретінде критерийлер жиынтығын көрсете аласыз. Критерийлерге сәйкес орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасының конфигурациясында қолдана аласыз.

Қолмен толықтырылатын бағдарламалар санатын жасау үшін:

1. Консоль ағашында **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарлама санаттары** ішкі қалтасын таңдаңыз.
2. **Жаңа санат** түймесін басыңыз.

   Жаңа санат шебері шеберін іске қосыңыз. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Санат түрі** шебері терезесінде **Қолмен толықтырылатын санат** пайдаланушы санатының түрін таңдаңыз.
4. **Бағдарлама санатының атауын енгізу** шебері бетінде бағдарлама санатының жаңа атауын енгізіңіз.
5. **Бағдарламаларды санаттарға қосу шарттарын конфигурациялау** бетінде **Қосылуда** түймесін басыңыз.
6. Ашылмалы тізімнен өзіңізге қажетті параметрлерді белгілеңіз:

   - **Орындалатын файлдардың тізімінен**

     Осы нұсқа таңдалған болса, санатқа қосылатын бағдарламаларды клиент құрылғысындағы орындалатын файлдар тізімінен таңдауға болады.

- **Файлдың сипаттарынан**

  Осы нұсқа таңдалған болса, бағдарламалардың пайдаланушы санатына қосылатын орындалатын файлдардың мәліметтер өрістерін қолмен көрсетуге болады.

- **Қалта файлдарының метадеректері**

  Клиент құрылғысында орындалатын файлдарды қамтитын қалтаны көрсетіңіз. Көрсетілген қалтаға кіретін орындалатын файлдардың метадеректері Басқару серверіне жіберіледі. Осындай метадеректері бар орындалатын файлдар бағдарламалардың пайдаланушы санатына қосылады.

- **Қалтадағы файлдардың бақылау сандары**

  Осы нұсқа таңдалған болса, клиент құрылғысында қалтаны таңдауға немесе жасауға болады. Көрсетілген қалтадағы MD5 файлдары хеш-функциясы Басқару серверіне жіберіледі. Көрсетілген қалтадағыдай хеші бар бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

- **Қалтадағы файлдардың сертификаттары**

  Осы нұсқа таңдалған болса, сертификаттармен қол қойылған орындалатын файлдары бар клиент құрылғысындағы қалтаны көрсетуге болады. Орындалатын файлдардың сертификаттары оқып салыстырылады және санаттың шарттарына қосылады. Көрсетілген сертификаттарға сай қол қойылған орындалатын файлдар пайдаланушы санатына қосылады.

  > Сертификаттар туралы ақпаратты тек PE форматындағы (.exe, .dll, .sys) орындалатын файлдардан алуға болады.

- **MSI орнатқышының файлдарының метадеректері**

  Осы нұсқа таңдалған болса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде MSI орнатушы файлын көрсетуге болады. Бағдарлама орнатушының метадеректері Басқару серверіне жіберілетін болады. Орнатушының метадеректері көрсетілген MSI орнатушысына сай келетін бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

- **Бағдарламаның MSI орнатушысының файлдарының бақылау сомалары**

  Осы нұсқа таңдалған болса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде MSI орнатушы файлын көрсетуге болады. Бағдарлама орнатушы файлдарының хеші Басқару серверіне жіберілетін болады. MSI орнатушысы файлдарының хеші көрсетілген мәнге сай келетін бағдарламалар, бағдарламалардың пайдаланушы санатына қосылатын болады.

- **KL санатынан**

  Осы нұсқа таңдалған болса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде Kaspersky бағдарламалары санатын қосуға болады. Көрсетілген KL санатына кіретін бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

- **Қолданба жолын көрсету (қолдау көрсетілетін маскалар)**

  Осы нұсқа таңдалса, орындалатын файлдары бағдарламалардың пайдаланушы санаттарына қосылатын клиент құрылғысындағы файлды немесе қалтаны көрсетуге болады. *C:\path_to_exe** сияқты тұрақты өрнектерді пайдалануға болады, мысалы: *C:\Program Files\Internet Explorer**.

- **Репозиторийден сертификатты таңдау**

  Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Санат шарты көрсетілген сертификатпен қол қойылған орындалатын файлдарға ғана сәйкес келеді.

Түгендеу тапсырмасын жасап, іске қоссаңыз немесе Kaspersky Endpoint Security саясатында **Іске қосылған қолданбалар** туралы құсбелгісін таңдасаңыз, сертификаттар қоймаға қосылады. Сіз екі әрекетті де орындай аласыз.

Сертификаттар туралы ақпаратты тек PE форматындағы (.exe, .dll, .sys) орындалатын файлдардан алуға болады.

- **Тасушының түрі**

  Осы нұсқа таңдалған болса, бағдарлама іске қосылатын тасушының түрін (кез келген немесе алынбалы диск) көрсетуге болады. Таңдалған типтегі тасушыда іске қосылатын бағдарламалар бағдарламалардың пайдаланушы санатына қосылады.

7. **Бағдарлама санатын жасау** шеберінің бетінде **Аяқтау** түймесін басыңыз.

Kaspersky Security Center бағдарламасы сандық қолтаңбаны қамтитын файлдардағы метадеректермен ғана жұмыс істейді. Сандық қолтаңбалары жоқ файлдардың метадеректері негізінде санатты жасау мүмкін емес.

Шебердің жұмысы нәтижесінде, қолмен толықтырылатын бағдарламалардың пайдаланушы санаты жасалады. Жасалған санатты **Бағдарлама санаттары** қалтасының жұмыс аймағындағы санаттар тізімінде қарауға болады.

Қолданба санатын KLC файлына экспорттағыңыз келсе, санат атауын тінтуірдің оң жақ түймесімен басып, мәзірден **Экспорттау** опциясын таңдаңыз, содан кейін ашылатын терезеде файл атауын көрсетіңіз де, **Сақтау** түймесін басыңыз.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау

Құрылғыдан орындалатын файлдарды, іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдардың үлгісі ретінде пайдалануға болады. Таңдалған құрылғылардағы орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Құрылғылардан орындалатын файлдар тізімін алу үшін:

1. Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Linux саясаты жасалды және белсенді екеніне көз жеткізіңіз. Саясатта Қолданбаны басқару құрамдас бөлігін қосыңыз.

2. Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын құру үшін:

1. Консоль ағашында **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарлама санаттары** ішкі қалтасын таңдаңыз.

2. **Жаңа санат** түймесін басыңыз.

   Жаңа санат шебері шеберін іске қосыңыз. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Шебердің **Санат түрі** бетінде **Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санаты** пайдаланушы санаты түрін таңдаңыз.

4. **Бағдарлама санатының атауын енгізу** шебері бетінде бағдарлама санатының жаңа атауын енгізіңіз.

5. **Параметрлер** шеберінің бетінде **Қосу** түймесін басыңыз.

6. Бағдарламалар санатын құру үшін орындалатын файлдары пайдаланылатын құрылғыны немесе құрылғыларды таңдаңыз.

7. Келесі параметрлерді белгілеңіз:

   - **Хеш функциясын есептеп шығару алгоритмі**

     Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

     SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы SHA256 хеш функциясын есептеп шығаруды қолдайды. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен нұсқалар үшін қолдау көрсетіледі.

     Санат файлдары үшін Kaspersky Security Center бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

     - Желіңізде орнатылған қауіпсіздік бағдарламаларының барлық даналары Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы болса, онда **SHA256** жалаушасын қойыңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен бағдарлама нұсқалары үшін, орындалатын файлдың SHA256 өлшемшарты бойынша жасалған санатты қосу ұсынылмайды. Бұл қауіпсіздік бағдарламаның істен шығуына әкелуі мүмкін. Бұл жағдайда, санат файлдары үшін MD5 криптографиялық хеш функциясын қолдана аласыз.

     - Сіздің желіңізде Kaspersky Endpoint Security 10 Service Pack 2 for Windows бағдарламасының ең ерте нұсқалары орнатылған болса, **MD5 хэші** тармағын таңдаңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқалары үшін орындалатын файлдың MD5 бақылау сомасының өлшемшарты бойынша жасалған санатты қосуға болмайды. Бұл жағдайда, санат файлдары үшін SHA256 криптографиялық хеш функциясын қолдана аласыз.

     Желіңіздегі әртүрлі құрылғылар Kaspersky Endpoint Security 10 бағдарламасының ең ерте нұсқаларын да, ең кейінгі нұсқаларын да қолданса, онда **SHA256** жалаушасы мен **MD5 хэші** жалаушасын қойыңыз.

     Әдепкі бойынша, **Санаттағы файлдар үшін SHA256 есептеп шығару (Kaspersky Endpoint Security 10 Service Pack 2 for Windows үшін қолдау көрсетіледі)** жалаушасы қойылған.

     Әдепкі бойынша, **Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)** алынып тасталған.

   - **Басқару серверінің қоймасымен деректерді синхрондау**

     Басқару сервері көрсетілген қалтада (немесе қалталарда) өзгерістерді мезгіл-мезгіл тексеріп отыруын қаласаңыз, осы параметрді таңдаңыз.

     Әдепкі бойынша, параметр өшірулі.

     Егер сіз осы параметрді қоссаңыз, көрсетілген қалтада (қалталарда) өзгерістерді тексеру үшін кезеңді (сағатпен) көрсетіңіз. Әдепкі бойынша, тексеру кезеңі 24 сағатқа тең келеді.

8. Шебердің **Сүзгі** бетінде келесі параметрлерді көрсетіңіз:

   - **Файл түрі**

     Бұл бөлімде бағдарламалар санатын құру үшін қолданылатын файл түрін көрсетуге болады.

     Барлық файлдар. Жасалып жатқан санат үшін барлық файлдар ескеріледі. Әдепкі бойынша, осы нұсқа таңдалған.

     Тек бағдарлама санаттарынан тыс файлдар. Құрылған санат үшін тек бағдарлама санаттарынан тыс файлдар ескеріледі.

   - **Қалталар**

     Бұл бөлімде бағдарламалар санатын құру үшін пайдаланылатын файлдары бар таңдалған құрылғылардың қалталарын көрсетуге болады.

     Барлық қалталар. Жасалып жатқан санат үшін барлық қалталар ескеріледі. Әдепкі бойынша, осы нұсқа таңдалған.

     Көрсетілген қалта. Жасалып жатқан санат үшін тек көрсетілген қалта ескеріледі. Егер сіз осы параметрді таңдасаңыз, қалта жолын көрсетуіңіз керек.

9. **Бағдарлама санатын жасау** шеберінің бетінде **Аяқтау** түймесін басыңыз.

Шебер аяқталғаннан кейін, реттелмелі бағдарламалар санаттары құрылады. Жасалған санатты **Бағдарлама санаттары** қалтасының жұмыс аймағындағы санаттар тізімінде қарауға болады.

Қолданба санатын KLC файлына экспорттағыңыз келсе, санат атауын тінтуірдің оң жақ түймесімен басып, мәзірден **Экспорттау** опциясын таңдаңыз, содан кейін ашылатын терезеде файл атауын көрсетіңіз де, **Сақтау** түймесін басыңыз.

Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау

Таңдалған қалталардың орындалатын файлдарын, ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдардың эталондық жиынтығы ретінде пайдалануға болады. Таңдалған қалталардағы орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру үшін:

1. Консоль ағашында **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарлама санаттары** ішкі қалтасын таңдаңыз.

2. **Жаңа санат** түймесін басыңыз.

   Жаңа санат шебері шеберін іске қосыңыз. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Шебердің **Санат түрі** бетінде **Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санаты** пайдаланушы санаты түрін таңдаңыз.

4. **Бағдарлама санатының атауын енгізу** шебері бетінде бағдарлама санатының жаңа атауын енгізіңіз.

5. **Қойма қалтасы** шеберінің бетінде **Шолу** түймесін басыңыз.

6. Орындалатын файлдары бағдарламалар санатын құру үшін пайдаланылатын қалтаны көрсетіңіз.

7. Келесі параметрлерді конфигурациялаңыз:

- **Санатқа динамикалық түрде қосылатын кітапханаларды (DLL) қосу**

  Бағдарламалар санатына динамикалық түрде қосылатын кітапханалар (DLL пішіміндегі файлдар) қосылады және Бағдарламаны басқару құрамдасы жүйеде іске қосылған осындай кітапханалардың әрекеттерін тіркейді. DLL пішіміндегі файлдарды санатқа қосу кезінде Kaspersky Security Center жұмысының өнімділігі төмендеуі мүмкін.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Санатқа скрипт туралы деректерді қосу**

  Бағдарлама санатына скрипт туралы деректер қосылады және скрипттер Веб-қауіптен қорғаныс құрамдасы тарапынан бұғатталмайды. Скрипт туралы деректерді санатқа қосу кезінде Kaspersky Security Center жұмысының өнімділігі төмендеуі мүмкін.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Хэш функциясын есептеу алгоритмі**: **Осы санаттағы файлдар үшін SHA256 мәнін есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан кейінгі нұсқаларында қолдау көрсетіледі) / Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)**

  Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

  SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы SHA256 хеш функциясын есептеп шығаруды қолдайды. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен нұсқалар үшін қолдау көрсетіледі.

  Санат файлдары үшін Kaspersky Security Center бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

  - Желіңізде орнатылған қауіпсіздік бағдарламаларының барлық даналары Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы болса, онда **SHA256** жалаушасын қойыңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен бағдарлама нұсқалары үшін, орындалатын файлдың SHA256 өлшемшарты бойынша жасалған санатты қосу ұсынылмайды. Бұл қауіпсіздік бағдарламаның істен шығуына әкелуі мүмкін. Бұл жағдайда, санат файлдары үшін MD5 криптографиялық хеш функциясын қолдана аласыз.

  - Сіздің желіңізде Kaspersky Endpoint Security 10 Service Pack 2 for Windows бағдарламасының ең ерте нұсқалары орнатылған болса, **MD5 хэші** тармағын таңдаңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқалары үшін орындалатын файлдың MD5 бақылау сомасының өлшемшарты бойынша жасалған санатты қосуға болмайды. Бұл жағдайда, санат файлдары үшін SHA256 криптографиялық хеш функциясын қолдана аласыз.

  Желіңіздегі әртүрлі құрылғылар Kaspersky Endpoint Security 10 бағдарламасының ең ерте нұсқаларын да, ең кейінгі нұсқаларын да қолданса, онда **SHA256** жалаушасы мен **MD5 хэші** жалаушасын қойыңыз.

  Әдепкі бойынша, **Санаттағы файлдар үшін SHA256 есептеп шығару (Kaspersky Endpoint Security 10 Service Pack 2 for Windows үшін қолдау көрсетіледі)** жалаушасы қойылған.

  Әдепкі бойынша, **Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)** алынып тасталған.

- **Қалтада өзгертулер бар-жоғын мәжбүрлеп сканерлеу**

  Егер бұл параметр қосулы болса, бағдарлама санаттарды толықтыру қалтасында өзгертулердің бар-жоғын мезгіл-мезгіл мәжбүрлеп тексереді. Тексерудің сағат түріндегі мерзімділігін жалаушаның жанындағы енгізу өрісінде көрсетуге болады. Әдепкі бойынша, мәжбүрлеп тексеру кезеңі 24 сағатқа тең келеді.

  Осы параметр өшірулі болса, қалтаны мәжбүрлеп тексеру орындалмайды. Сервер қалтадағы файлдарды өзгерту, қосу немесе жою кезінде оларға жүгінеді.

  Әдепкі бойынша, параметр өшірулі.

8. **Бағдарлама санатын жасау** шеберінің бетінде **Аяқтау** түймесін басыңыз.

Шебер аяқталғаннан кейін, реттелмелі бағдарламалар санаттары құрылады. Жасалған санатты **Бағдарлама санаттары** қалтасының жұмыс аймағындағы санаттар тізімінде қарауға болады.

Қолданба санатын KLC файлына экспорттағыңыз келсе, санат атауын тінтуірдің оң жақ түймесімен басып, мәзірден **Экспорттау** опциясын таңдаңыз, содан кейін ашылатын терезеде файл атауын көрсетіңіз де, **Сақтау** түймесін басыңыз.

Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу

Бағдарламаны іске қосуға тыйым салынған және **Бағдарламаны сынақ режимінде іске қосуға тыйым салынған** оқиғаларымен байланысты орындалатын файлдарды қолмен толықтырылатын қолданыстағы бағдарламалар санатына немесе жаңа бағдарламалар санатына қоса аласыз.

Қолданбаны басқару оқиғаларымен байланысты орындалатын файлдарды қолданба санатына қосу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.

2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.

3. **Оқиғалар** қойыншасында өзіңізге қажетті оқиғаны таңдаңыз.

4. Оқиғаның контекстік мәзірінен **Санатқа қосу** тармағын таңдаңыз.

5. Ашылған **Оқиғаға қатысты орындалатын файл бойынша әрекет** терезесінде қажетті параметрлерді белгілеңіз:

   Келесі нұсқалардың бірін таңдаңыз:

   - **Жаңа бағдарлама санатына қосу**

     Бағдарламалар санатын жасағыңыз келсе, осы нұсқаны таңдаңыз.

     ОК түймесі арқылы жаңа санат шеберін іске қосыңыз. Шебер жұмысының нәтижесінде, көрсетілген параметрлері бар санат жасалатын болады.

     Әдепкі бойынша нұсқа таңдалмаған.

   - **Қолданыстағы бағдарлама санатына қосу**

     Ережелерді қолданыстағы бағдарламалар санатына қосу керек болса, осы нұсқаны таңдаңыз. Бағдарламалар санаттары тізіміндегі қажетті санатты таңдаңыз.

     Әдепкі бойынша, осы нұсқа таңдалады.

Ереже түрі блогында келесі параметрлерді таңдаңыз:

- **Санатқа қосу**

  Ережелерді бағдарлама санаттары шарттарына қосу үшін осы нұсқаны таңдаңыз.

  Әдепкі бойынша, осы нұсқа таңдалады.

- **Шығарылатындарға қосу ережелері**

  Ережелерді бағдарлама санаттарын алып тастағыңыз келсе, осы нұсқаны таңдаңыз.

Файл ақпаратының түрі блогында келесі параметрлердің бірін таңдаңыз:

- **Сертификат мәліметтері немесе сертификаты жоқ файлдар үшін SHA256 хэштері**

  Файлдарға сертификат арқылы қол қоюға болады. Бұл арада, бір сертификатпен бірнеше файлға қол қоюға болады. Мысалы, бір бағдарламаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі бағдарламаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа бағдарламаның бірнеше нұсқасы немесе бір өндірушінің бірнеше бағдарламасы кіруі мүмкін.

  Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

  Санат ережелеріне орындалатын файл сертификатының деректерін немесе сертификаты жоқ файлдар үшін SHA256 хэш функциясын қосу қажет болса, осы нұсқаны таңдаңыз.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сертификат мәліметтері (сертификаты жоқ файлдар өткізіп жіберіледі)**

  Файлдарға сертификат арқылы қол қоюға болады. Бұл арада, бір сертификатпен бірнеше файлға қол қоюға болады. Мысалы, бір бағдарламаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі бағдарламаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа бағдарламаның бірнеше нұсқасы немесе бір өндірушінің бірнеше бағдарламасы кіруі мүмкін.

  Санат ережелеріне орындалатын файл сертификатының деректерін қосу қажет болса, осы нұсқаны таңдаңыз. Орындалатын файлдың сертификаты болмаса, ондай файлды өткізіп жіберуге болады. Ол туралы ақпарат санатқа қосылмайды.

- **Тек SHA256 (хэш жоқ файлдар өткізіп жіберіледі)**

  Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

  Санат ережелеріне тек орындалатын файлдың SHA256 хеш функциясының деректерін ғана қосу керек болса, осы нұсқаны таңдаңыз.

- **MD5 (ескірген режим, тек Kaspersky Endpoint Security 10 Service Pack 1 нұсқалары үшін ғана)**

  Әрбір файлдың өзіндік бірегей MD5 хэш функциясы бар. MD5 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

  Санат ережелеріне тек орындалатын файлдың MD5 хеш функциясының деректерін ғана қосу керек болса, осы нұсқаны таңдаңыз. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 1 for Windows және одан да төмен нұсқалар үшін қолдау көрсетіледі.

6. **OK** түймесін басыңыз.

Клиент құрылғыларында бағдарламалардың іске қосылуын басқаруды конфигурациялау

Бағдарламаларды санаттау құрылғылардағы бағдарламалардың іске қосылуын басқару процесін оңтайландыруға мүмкіндік береді. Сіз бағдарламалар санатын құра аласыз және саясат бағдарламаларын басқару құрамдасын осы саясат қолданылатын құрылғыларда тек аталған санаттағы бағдарламалар жұмыс істейтін етіп конфигурациялай аласыз. Мысалы, *Бағдарлама_1* және *Бағдарлама_2* бағдарламаларын қамтитын санатты жасадыңыз. Осы санатты саясатқа қосқаннан кейін, осы саясат қолданылған құрылғыларда тек *Бағдарлама_1* және *Бағдарлама_2* бағдарламаларын ғана іске қосуға рұқсат етіледі. Егер пайдаланушы санатқа кірмейтін бағдарламаны, мысалы, *Бағдарлама_3* бағдарламасын іске қосуға тырысса, онда мұндай бағдарламаны іске қосу бұғатталады. Пайдаланушыға Бағдарламаны басқару ережесіне сәйкес *Бағдарлама_3* бағдарламасын іске қосуға тыйым салынғаны туралы хабар көрсетіледі. Сіз көрсетілген қалтаға кіретін әртүрлі критерийлер негізінде автоматты түрде толықтырылатын санат жасай аласыз. Бұл жағдайда, файлдар көрсетілген қалтадан санатқа автоматты түрде қосылады. Бағдарламалардың орындалатын файлдары көрсетілген қалтаға көшіріледі, автоматты түрде өңделеді және олардың метрикалары санатқа енгізіледі.

Клиент құрылғыларында бағдарламалардың іске қосылуын басқаруды конфигурациялау үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарлама санаттары** салынған қалтасын таңдаңыз.

2. **Бағдарлама санаттары** қалтасының жұмыс аймағында іске қосылуын басқарғыңыз келетін бағдарлама санаттарын жасаңыз.

3. Kaspersky Endpoint Security for Windows үшін жаңа саясат жасау мақсатында **Басқарылатын құрылғылар** қалтасының **Саясаттар** қойындысындағы **Жаңа саясат** түймесін басып, шебердегі нұсқауларды орындаңыз.

   Егер мұндай саясат бұрыннан бар болса, бұл қадамды өткізіп жіберуге болады. Аталған санаттағы бағдарламалардың іске қосылуын басқару осы саясаттың параметрлерінде конфигурациялануы мүмкін. Жасалған саясат **Басқарылатын құрылғылар** қалтасында, **Саясаттар** қойыншасында көрсетіледі.

4. Kaspersky Endpoint Security for Windows бағдарламасы үшін саясаттың контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Kaspersky Endpoint Security for Windows саясаты сипаттары терезесі ашылады.

5. Kaspersky Endpoint Security for Windows саясаты сипаттары терезесінде, **Қауіпсіздікті бақылау** → **Бағдарламаны басқару** бөлімінде **Бағдарламаны басқару** жалаушасын қойыңыз.

6. **Қосу** түймесін басыңыз.

   Бағдарламаны басқару ережесі терезесі ашылады.

7. **Бағдарламаны басқару ережесі** терезесінде **Санат** ашылмалы тізімінде іске қосу ережесі қолданылатын бағдарламалар санатын таңдаңыз. Таңдалған бағдарлама санаты үшін іске қосу ережесінің параметрлерін конфигурациялаңыз.

   Kaspersky Endpoint Security for Windows 10 Service Pack 2 және одан да жоғары нұсқасы үшін, орындалатын файлдың MD5 хэші критерийі бойынша жасалған санаттар, бағдарламалар көрсетілмейді.

   Kaspersky Endpoint Security 10 Service Pack 2 нұсқасынан төмен бағдарлама нұсқалары үшін, орындалатын файлдың SHA256 өлшемшарты бойынша жасалған санатты қосу ұсынылмайды. Бұл бағдарламаның ақауына әкелуі мүмкін.

Бақылау ережелерін конфигурациялау бойынша толығырақ нұсқаулар Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

8. **OK** түймесін басыңыз.

Аталған санатқа кіретін құрылғыларда бағдарламаларды іске қосу жасалған ережеге сәйкес орындалады. Жасалған ереже Kaspersky Endpoint Security for Windows саясаты сипаттары терезесінде, **Бағдарламаны басқару** бөлімінде көрсетіледі.

Орындалатын файлдарды іске қосу ережелерін статикалық талдау нәтижелерін қарау

Пайдаланушыларға қандай орындалатын файлдарды іске қосуға тыйым салынғаны туралы ақпаратты көру үшін:

1. **Басқарылатын құрылғылар** қалтасындағы консоль шежіресінен **Саясаттар** салынған қалтасын таңдаңыз.
2. Kaspersky Endpoint Security for Windows бағдарламасы үшін саясаттың контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Бағдарлама саясатының сипаттары терезесі ашылады.
3. Саясат сипаттары терезесіндегі **Бөлімдер** панелінде **Қауіпсіздікті бақылау** бөлімін, содан соң **Бағдарламаларды басқару** бөлікшесін таңдаңыз.
4. **Статикалық талдау** түймесін басыңыз.

   Қатынасу құқықтары тізімін талдау терезесі ашылады. Терезенің сол жағында Active Directory деректеріне негізделген пайдаланушылар тізімі көрсетіледі.
5. Пайдаланушы тізімінен таңдаңыз.

   Терезенің оң жағында сол пайдаланушыға тағайындалған бағдарламалардың санаттары көрсетіледі.
6. Пайдаланушыға іске қосуға тыйым салынған орындалатын файлдарды қарау үшін **Қатынасу құқықтары тізімін талдау** терезесінде **Файлдарды қарап шығу** түймесін басыңыз.

   Пайдаланушыға іске қосуға тыйым салынған орындалатын файлдардың тізімін көрсететін терезе ашылады.
7. Санатқа кіретін орындалатын файлдардың тізімін көру үшін бағдарламалар санатын таңдап, **Санат файлдарын қарап шығу** түймесін басыңыз.

   Ашылған терезеде бағдарламалар санатына кіретін орындалатын файлдардың тізімі көрсетіледі.

Бағдарламалар тізімдемелерін қарап шығу

Kaspersky Security Center бағдарламасы басқарылатын құрылғыларда орнатылған бағдарламалық жасақтаманы түгендейді.

Желілік агент Windows немесе Linux операциялық жүйесі бар құрылғыға орнатылған бағдарламалар тізімін құрастырады және тізімді басқару серверіне жібереді. Windows операциялық жүйесі бар клиент құрылғылары үшін Желілік агент орнатылған бағдарламалар туралы ақпараттың көп бөлігін Windows тізімдемесінен алады. Linux операциялық жүйесі бар клиент құрылғылары үшін орнатылған бағдарламалар туралы ақпаратты Желілік агент пакет диспетчерлерінен алады.

Клиент құрылғыларында орнатылған бағдарламалардың тізімдемесін көру үшін:

Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Бағдарламалар тізімдемесі** салынған қалтасын таңдаңыз.

Бағдарламалар тізімдемесі қалтасының жұмыс аймағында клиент құрылғылары мен Басқару серверінде орнатылған бағдарламалар тізімі көрсетіледі.

Осы бағдарламаның контекстік мәзірінен **Сипаттар** тармағын таңдау арқылы кез келген бағдарлама туралы егжей-тегжейлі мәліметтерді көруге болады. Бағдарлама сипаттары терезесінде бағдарлама туралы жалпы ақпарат және бағдарламаның орындалатын файлдары туралы ақпарат, сондай-ақ бағдарлама орнатылған құрылғылардың тізімі көрсетіледі.

Кез келген бағдарламаның контекстік мәзірінде сіз:

- бұл бағдарламаны бағдарламалар санатына қоса аласыз;
- бағдарламаға тег тағайындай аласыз;
- бағдарламалар тізімін CSV немесе TXT пішіміндегі файлдарға экспорттай аласыз;
- бағдарламаның сипаттарын, мысалы, өндірушінің аты, нұсқа нөмірі, орындалатын файлдар тізімі, бағдарлама орнатылған құрылғылар тізімі, қолжетімді бағдарламалық жасақтама жаңартуларының тізімі немесе анықталған бағдарламалық жасақтама осалдықтарының тізімін қарап шыға аласыз.

Белгілі бір критерийлерге сәйкес келетін бағдарламаларды көру үшін сіз **Бағдарламалар тізімдемесі** қалтасының жұмыс аймағындағы сүзу өрістерін пайдалана аласыз.

Бағдарламалар тізімдемесі бөліміндегі таңдалған құрылғылар сипаттары терезесінде сіз құрылғыда орнатылған бағдарламалар тізімін көре аласыз.

Орнатылған бағдарламалар туралы есеп жасау

Бағдарламалар тізімдемесі қалтасының жұмыс аймағында сіз орнатылған бағдарламалар туралы ақпаратты, соның ішінде әр бағдарлама орнатылған құрылғылардың санын қамтитын есепті жасау үшін **Орнатылған бағдарламалар туралы есепті көру** түймесін басуға болады. **Орнатылған бағдарламалар туралы есеп** бетінде ашылатын есепте Kaspersky бағдарламалары туралы және үшінші тарап бағдарламалары туралы ақпарат бар. Егер сізге тек клиент құрылғыларында орнатылған Kaspersky бағдарламалары туралы ақпарат қажет болса, **Жиынтық ақпарат** тізімінен Kaspersky тармағын таңдаңыз.

Kaspersky бағдарламалары, сондай-ақ қосалқы және виртуалды Басқару серверлеріне қосылған құрылғылардағы басқа өндірушілер бағдарламалары туралы ақпарат дәл солай негізгі Басқару сервері бағдарламаларының тізімдемесінде сақталады. Қосалқы және виртуалды Серверлерден алынған деректерді қосқаннан кейін **Орнатылған бағдарламалар туралы есепті көру** түймесін бассаңыз, ашылған **Орнатылған бағдарламалар туралы есеп** бетінде бұл ақпаратты көре аласыз.

Қосалқы және виртуалды Басқару серверлерінен алынған ақпаратты орнатылған бағдарламалар туралы есепке қосу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар тораптыны таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.

3. **Есептер** қойындысында **Орнатылған бағдарламалар туралы есеп** таңдаңыз.

4. Есептің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Сипаттар: **Орнатылған бағдарламалар туралы есеп** терезесі ашылады.

5. **Басқару серверлерінің иерархиясы** бөлімінде **Қосалқы және виртуалды Басқару серверлерінен алынған деректерді қамту** жалаушасын қойыңыз.

6. **OK** түймесін басыңыз.

Нәтижесінде, қосалқы және виртуалды Басқару серверлерінен алынған ақпарат **Орнатылған бағдарламалар туралы есеп** тармағына енгізіледі.

Бағдарламалық жасақтаманы түгендеудің басталу уақытын өзгерту

Kaspersky Security Center бағдарламасы, Windows операциялық жүйесінің басқаруымен жұмыс істейтін басқарылатын клиент құрылғыларында орнатылған бағдарламалық жасақтаманы түгендейді.

Желілік агент құрылғыда орнатылған бағдарламалар тізімін құрастырып, тізімді Басқару серверіне жібереді. Желілік агент орнатылған бағдарламалар туралы ақпаратты Windows тізімдемесінен автоматты түрде алады.

Құрылғының ресурстарын сақтау үшін, әдепкі бойынша Желілік агент орнатылған бағдарламалар туралы ақпаратты Желілік агент қызметі іске қосылғаннан кейін 10 минуттан соң ала бастайды.

Желілік агент қызметі іске қосылғаннан кейін құрылғының бағдарламалық жасақтамасын түгендей бастау уақытын өзгерту үшін:

1. Желілік агент орнатылған құрылғының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.

2. Келесі бөлімге өтіңіз:

   - 32 разрядты жүйе үшін:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - 64 разрядты жүйе үшін:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF

3. KLINV_INV_COLLECTOR_START_DELAY_SEC кілті үшін өзіңізге қажетті секундтардағы мәнді белгілеңіз.

   Әдепкі бойынша, 600 секунд мәні көрсетілген.

4. Желілік агент қызметін қайта іске қосыңыз.

Нәтижесінде, Желілік агент қызметін іске қосқаннан кейін бағдарламалық жасақтаманы түгендей бастау уақыты өзгертіледі.

Лицензиялы бағдарламаларда лицензиялық кілттерді басқару туралы

Kaspersky Security Center басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламалары үшін лицензиялық кілттердің қолданылуын бақылауға мүмкіндік береді. Лицензиялық кілтті пайдалануды бақылауға болатын бағдарламалардың тізімі бағдарламалар тізімдемесінен алынады. Әрбір лицензиялық кілт үшін келесі шектеулердің бұзылуын көрсетуге және бақылауға болады:

- Осы лицензиялық кілтті пайдаланатын бағдарлама орнатылатын құрылғылардың ең көп саны.
- Лицензиялық кілттің қолданылу мерзімінің аяқталу күні.

Kaspersky Security Center бағдарламасы сіз нақты лицензиялық кілтті көрсеткеніңізді тексермейді. Сіз көрсеткен шектеулерді ғана бақылай аласыз. Лицензиялық кілтке қойылған шектеулердің бірі бұзылған жағдайда, Басқару сервері ақпараттық, ескерту немесе функционалдық ақау оқиғасын тіркейді.

Лицензиялық кілттер бағдарлама топтарына байланған. Бағдарламалар тобы – бұл бір критерий немесе бірнеше критерий негізінде біріктірілетін үшінші тарап бағдарламаларының тобы. Бағдарламаларды бағдарлама атауы, бағдарлама нұсқасы, өндіруші және тег бойынша анықтауға болады. Егер критерийлердің кем дегенде біреуі орындалса, бағдарлама топқа қосылады. Бағдарламалардың әр тобына бірнеше лицензиялық кілтті қосуға болады, бірақ әрбір лицензиялық кілт тек бір бағдарлама тобына қосылуы мүмкін.

Сондай-ақ, лицензиялық кілттердің қолданылуын бақылау үшін лицензиялы бағдарламалар топтарының күйі туралы есепті пайдалануға болады. Бұл есепте лицензиялы бағдарламалар топтарының ағымдағы жағдайы туралы ақпарат берілген, соның ішінде:

- Бағдарламалардың әрбір тобына лицензиялық кілттерді орнату саны.
- Пайдаланылатын лицензиялық кілттер мен еркін лицензиялық кілттердің саны.
- Басқарылатын құрылғыларда орнатылған лицензиялы бағдарламалардың тізімі.

Үшінші тарап бағдарламаларында лицензиялық кілтті басқаруға арналған құралдар **Үшінші тарап лицензияларын пайдалану** (**Кеңейтілген → Бағдарламаларды басқару → Үшінші тарап лицензияларын пайдалану**) қалтасында орналасқан. Бұл қалтада сіз бағдарламалар топтарын жасай аласыз, лицензиялық кілттерді қоса аласыз және лицензияланған бағдарламалар топтарының күйі туралы есепті құрастыра аласыз.

Үшінші тарап бағдарламаларының лицензиялық кілттерін басқару құралдары **Интерфейсті конфигурациялау** терезесінде Осалдықтар мен патчтарды басқару параметрін қосқан жағдайда ғана қолжетімді.

Лицензиялы бағдарламалар тобын жасау

Лицензиялы бағдарламалар тобын жасау үшін:

1. Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Үшінші тарап лицензияларын пайдалану** салынған қалтасын таңдаңыз.
2. **Лицензиялы бағдарламалар тобын қосу** түймесі бойынша Лицензиялы бағдарламалар тобын қосу шебері іске қосыңыз.

   Лицензиялы бағдарламалар тобын қосу шебері іске қосылды.

3. **Лицензиялы бағдарламалар тобының мәліметтері** қадамында бағдарламалар тобына қандай бағдарламаларды қосқыңыз келетінін көрсетіңіз:

   - **Лицензиялы бағдарламалар тобының атауы**

   - **Шектеулерді бұзуды бақылау**

     Бағдарламалар тобының лицензиялық кілтіне қойылған шектеулердің бірі бұзылған жағдайда, Басқару сервері ақпараттық, ескерту немесе функционалдық ақау оқиғасын тіркейді:

     - Ақпараттық оқиға: **Лицензиялы бағдарламалар топтарының біреуі үшін рұқсат етілген орнатулардың саны (95%-дан) асты**.

     - Ескерту оқиғасы: **Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі жақын арада асырылады**.

     - Функционалдық ақау: **Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі асырылды**.

       Оқиға шартты орындау кезінде бір рет қана тіркеледі. Келесі жолы дәл осы оқиғаны орнату саны қалыпты деңгейге оралғанда ғана тіркеуге болады, содан кейін оқиға қайтадан орын алады. Оқиғаны сағатына бір реттен артық тіркеу мүмкін емес.

   - **Анықталған бағдарламаларды лицензиялы бағдарламалардың осы тобына қосу критерийлері**

     Бағдарламалар тобына қандай бағдарламаларды қосқыңыз келетінін анықтау үшін критерийлерді көрсетіңіз. Бағдарламаларды бағдарлама атауы, бағдарлама нұсқасы, өндіруші және тег бойынша анықтауға болады. Сіз кем дегенде бір критерийді көрсетуіңіз керек. Егер критерийлердің кем дегенде біреуі орындалса, бағдарлама топқа қосылады.

4. **Қолданыстағы лицензиялық кілттер туралы деректерді енгізу** қадамында бақылағыңыз келетін лицензия кілттерін көрсетіңіз. **Белгіленген лицензиялық шектеулердің бұзылуын басқару** параметрін таңдап, лицензиялық кілттерді қосыңыз:

   a. **Қосу** түймесін басыңыз.

   b. Қосу қажет лицензиялық кілтті таңдап, **ОК** түймесін басыңыз. Егер қажетті лицензиялық кілт тізімде болмаса, **Қосу** түймесін басып, лицензиялық кілттің сипаттарын көрсетіңіз.

5. **Лицензиялы бағдарламалар тобын қосу** қадамында **Дайын** түймесін басыңыз.

Лицензиялы бағдарламалар тобы жасалып, **Үшінші тарап лицензияларын пайдалану** қалтасында көрсетіледі.

Лицензиялы бағдарламалар топтары үшін лицензиялық кілттерді басқару

Лицензиялы бағдарламалар тобына лицензиялық кілт жасау үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Үшінші тарап лицензияларын пайдалану** салынған қалтасын таңдаңыз.

2. **Үшінші тарап лицензияларын пайдалану** қалтасының жұмыс аймағындағы **Лицензиялы бағдарламалардың лицензиялық кілттерін басқару** түймесін басыңыз.

   Лицензияланған бағдарламаларда лицензиялық кілтті басқару терезесі ашылады.

3. **Лицензияланған бағдарламаларда лицензиялық кілтті басқару** терезесінде **Қосылуда** түймесін басыңыз.

   Лицензиялық кілт терезесі ашылады.

4. **Лицензиялық кілт** терезесінде лицензиялық кілттің сипаттарын және осы лицензиялық кілт лицензиялы бағдарламалар тобына қоятын шектеулерді көрсетіңіз.

   - **Атауы**. Лицензиялық кілт нөмірі.
   - **Пікір**. Таңдалған лицензиялық кілтке ескертпелер.
   - **Шектеу**. Осы лицензиялық кілтті пайдаланатын бағдарлама орнатылатын құрылғылардың саны.
   - **Мерзімі бітеді**. Лицензиялық кілттің қолданылу мерзімінің аяқталу күні.

Жасалған лицензиялық кілттер **Лицензияланған бағдарламаларда лицензиялық кілтті басқару** терезесінде көрсетіледі.

Лицензиялы бағдарламалар тобына лицензиялық кілтті қолдану үшін:

1. Консоль ағашында, **Кеңейтілген → Бағдарламаларды басқару** қалтасында **Үшінші тарап лицензияларын пайдалану** салынған қалтасын таңдаңыз.
2. **Үшінші тарап лицензияларын пайдалану** қалтасында лицензиялық кілтті қолданғыңыз келетін лицензиялы бағдарламалар тобын таңдаңыз.
3. Лицензиялы бағдарламалар тобының контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Лицензиялы бағдарламалар тобы сипаттары терезесі ашылады.

4. Лицензиялы бағдарламалар тобы сипаттары терезесінде **Лицензиялық кілттер** бөлімінде **Белгіленген лицензиялық шектеулердің бұзылуын басқару** нұсқасын таңдаңыз.
5. **Қосу** түймесін басыңыз.

   Лицензия кілтін таңдау терезесі ашылады.

6. **Лицензия кілтін таңдау** терезесінде лицензиялы бағдарламалар тобына қолданғыңыз келетін лицензиялық кілтті таңдаңыз.
7. **OK** түймесін басыңыз.

Лицензиялық кілтте көрсетілген лицензиялы бағдарламалар тобына шектеулер таңдалған лицензиялы бағдарламалар тобына қолданылады.

Орындалатын файлдарды түгендеу

Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімін алуға болады. Орындалатын файлдарды түгендеу үшін түгендеу тапсырмасын жасау қажет.

Орындалатын файлдарды түгендеу функциясы келесі бағдарламалар үшін қолжетімді:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent және одан да жоғары

Бір құрылғыдан алынатын орындалатын файлдар саны 150 000-нан аса алмайды. Осы шектеуге жеткеннен кейін, Kaspersky Security Center жаңа файлдарды алмайды.

Бастамас бұрын, деректерді Басқару серверіне жіберу үшін Kaspersky Endpoint Security саясатында және Желілік агент саясатында бағдарламаларды іске қосу туралы хабарландыруларды қосыңыз.

Бағдарламаларды іске қосу туралы хабарландыруларды қосу үшін:

- Kaspersky Endpoint Security саясатының параметрлерін ашып, келесі әрекеттерді орындаңыз:
  1. **Жалпы параметрлер** → **Есептер және қоймалар** тармағына өту.
  2. **Деректерді Басқару серверіне жіберу** бөлімінде **Іске қосылатын бағдарламалар туралы** жалаушасын қойыңыз.
  3. Өзгерістерді сақтаңыз.
- Желілік агент саясатының параметрлерін ашып, келесі әрекеттерді орындаңыз:
  1. **Қоймалар** бөліміне өту.
  2. **Орнатылған бағдарламалардың мәліметтері** жалаушасын қойыңыз.
  3. Өзгерістерді сақтаңыз.

Клиент құрылғыларында орындалатын файлдарды түгендеу тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Тапсырмалар** қалтасының жұмыс аймағындағы **Жаңа тапсырма** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрін таңдау** шебері терезесінде **Kaspersky Endpoint Security** тапсырма түрін, содан соң **Түгендеу** тапсырмасы ішкі түрін таңдап, **Келесі** түймесін басыңыз.
4. Шебердің келесі қадамдарын орындаңыз.

Шебер жұмысының нәтижесінде, Kaspersky Endpoint Security үшін түгендеу тапсырмасы жасалады. Жасалған тапсырма **Тапсырмалар** қалтасының жұмыс аймағындағы тапсырмалар тізімінде көрсетіледі.

Түгендеу нәтижесінде құрылғыларда анықталған орындалатын файлдар тізімі **Орындалатын файлдар** қалтасының жұмыс аймағында көрсетіледі.

Түгендеу кезінде, бағдарлама MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR пішіміндегі орындалатын файлдарды, сондай-ақ HTML файлдарын анықтайды.

Орындалатын файлдар туралы ақпаратты қарау

Клиент құрылғыларында табылған барлық орындалатын файлдардың тізімін көру үшін,

Бағдарламаларды басқару қалтасындағы консоль шежіресінен **Орындалатын файлдар** салынған қалтасын таңдаңыз.

Орындалатын файлдар қалтасының жұмыс аймағында құрылғыларда іске қосылған немесе Windows жүйесіне арналған Kaspersky Endpoint Security түгендеу тапсырмасы жұмыс істеп тұрған кезде табылған орындалатын файлдардың тізімі көрсетіледі.

Белгілі бір критерийлерді қанағаттандыратын орындалатын файлдар туралы деректерді көру үшін сүзгілеуді қолдана аласыз.

Орындалатын файлдың сипаттарын көру үшін:

Файлдың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

Орындалатын файл туралы ақпаратты, сондай-ақ орындалатын файл бар құрылғылардың тізімін қамтитын терезе ашылады.

Бақылау және есеп беру

Бұл бөлімде, Kaspersky Security Center бағдарламасында есептермен жұмыс істеу және мониторинг жүргізу функциялары сипатталған. Бұл функциялар желіңіздің инфрақұрылымы, қорғаныс күйі, сондай-ақ статистика туралы мәлімет алуға мүмкіндік береді.

Kaspersky Security Center бағдарламасын орналастыру немесе оның жұмыс істеуі барысында мониторинг функцияларын және есеп параметрлерін конфигурациялауға болады.

- **Индикаторлар**

  Басқару консолінде Kaspersky Security Center және басқарылатын құрылғылардың ағымдағы күйін түс индикаторлары арқылы жылдам бағалауға болады.

- **Статистика**

  Қорғаныс жүйесінің және басқарылатын құрылғылардың күйі туралы статистикалық ақпарат конфигурацияланатын ақпараттық тақталар түрінде көрсетіледі.

- **Есептер**

  Есептер бұл ақпаратты файлға сақтау, электрондық пошта арқылы жіберу және басып шығару үшін ұйымыңыздың желісінің қауіпсіздігі туралы толық сандық ақпаратты алуға мүмкіндік береді.

- **Оқиғалар**

Оқиғаларды таңдау, экранда Басқару серверінің дерекқорынан таңдалған аталған оқиғалар жиынтығын көруге арналған. Осы оқиға түрлері келесі санаттар бойынша топтастырылған:

- Маңыздылық деңгейі: **Критикалық оқиғалар**, **Функциялық ақаулар**, **Ескертулер** және **Ақпараттық оқиғалар**.
- Уақыт: **Соңғы оқиғалар**.
- Түрі: **Пайдаланушылардың сұраулары** және **Аудит оқиғалары**.

Kaspersky Security Center Web Console интерфейсінде конфигурациялауға қолжетімді параметрлер негізінде пайдаланушы тарапынан айқындалған оқиғалар таңдауын жасай аласыз және көре аласыз.

Сценарий: Бақылау және есеп беру

Бұл бөлімде Kaspersky Security Center бағдарламасында бақылау және есеп беру конфигурациясы сценарийі берілген.

Алдын ала талаптар

Kaspersky Security Center бағдарламасын ұйымның желісіне орналастырғаннан кейін, сіз Kaspersky Security Center көмегімен желінің қауіпсіздік күйін мониторингтеуге және есептерді қалыптастыруға кірісе аласыз.

Кезеңдер

Ұйымның желісіндегі бақылау және есептермен жұмыс келесі кезеңдерден тұрады:

1. **Құрылғылардың күйлерін ауыстыруды конфигурациялау**

   Нақты жағдайларға байланысты құрылғыларға күй беруді анықтайтын параметрлермен танысыңыз. Осы параметрлерді өзгерту арқылы, сіз *Критикалық* немесе *Ескерту* маңызды деңгейлері бар оқиғалар санын өзгерте аласыз.

   Құрылғы күйін ауыстыруды орнатқан конфигурациялаған, жаңа параметрлер ұйымыңыздың ақпараттық қауіпсіздік саясатына қайшы келмейтініне және ұйымыңыздың желісіндегі маңызды қауіпсіздік оқиғаларына уақтылы жауап бере алатыныңызға көз жеткізіңіз.

2. **Клиент құрылғыларындағы оқиғалар туралы хабарландыру параметрлерін конфигурациялау**

   Ұйымның қажеттіліктеріне сәйкес клиент құрылғыларындағы оқиғалар туралы хабарландыруларды (электрондық пошта, SMS немесе орындалатын файлды іске қосу арқылы) конфигурациялаңыз.

3. **Қауіпсіздік желіңіздің Вирустық шабуыл оқиғасына жауабын өзгерту**

   Желінің жаңа оқиғаларға жауабын конфигурациялау үшін Басқару сервері сипаттарындағы шекті мәндерді өзгертуге болады. Белсендірілетін аса қатаң саясатты жасай аласыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасай аласыз.

4. **Статистикалық ақпаратпен жұмыс**

   Статистиканың көрсетілуін ұйымыңыздың қажеттіліктеріне сәйкес конфигурациялаңыз.

5. **Ұйымыңыздың желі қауіпсіздігі күйін қарау**

   Ұйымыңыздың желі қауіпсіздігінің күйін тексеру үшін келесі әрекеттердің кез келгенін орындауға болады:

   - **Басқару сервері** түйінінің жұмыс аймағында, **Статистика** қойыншасында **Қорғаныс күйі** екінші деңгейлі қойыншасын (бетін) ашыңыз және **Нақты уақыт режимінде қорғау күйі** ақпараттық тақтасын қараңыз.
   - Есепті жасау және қарау **Қорғаныс жағдайы туралы есеп**.
   - Есепті жасау және қарау **Қателер туралы есеп**.

6. **Қорғалмаған клиент құрылғыларын табу**

   Қорғалмаған клиент құрылғыларын табу үшін, **Басқару сервері** түйінінің жұмыс аймағына өтіңіз, **Статистика** қойыншасында **Қорғаныс күйі** екінші деңгейлі қойыншасын (бетін) ашыңыз және **Жаңа желілік құрылғыларды табу журналы** ақпараттық тақтасын қараңыз. Сондай-ақ **Қорғанысты орналастыру туралы есеп** жасап, қарауға да болады.

7. **Клиент құрылғылары қорғанысын тексеру**

   Клиент құрылғыларының қорғанысын тексеру үшін, **Басқару сервері** түйінінің жұмыс аймағына өтіңіз, **Статистика** қойыншасында **Орналастыру** тармағын немесе **Қауіптер статистикасы** екінші деңгейлі қойыншасын (бетін) ашыңыз және тиісті ақпараттық тақталарды қараңыз. Сондай-ақ **Критикалық оқиғалар** оқиғалар таңдауын бастап, қарай аласыз.

8. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын бағдарламалар жұмыс істеп тұрған кезде туындайтын оқиғалар туралы ақпарат клиент құрылғысынан беріледі және Басқару серверінің дерекқорында тіркеледі. Басқару серверіне түсетін жүктемені азайту үшін дерекқорда сақталуы мүмкін оқиғалардың ең көп санын бағалаңыз және шектеңіз.

   Дерекқордағы оқиғалар жүктемесін бағалау үшін, дерекқордағы орынды есептеңіз. Сондай-ақ, дерекқордың толып кетуін болдырмау үшін оқиғалардың ең көп санын шектей аласыз.

9. **Лицензия мәліметтерін қарау**

   Лицензия туралы ақпаратты қарап шығу үшін, **Басқару сервері** түйінінің жұмыс аймағына өтіңіз, **Статистика** қойыншасында **Орналастыру** екінші деңгейлі қойыншасын (бетін) ашыңыз және **Лицензиялық кілтті пайдалану** ақпараттық тақтасын қараңыз. Сондай-ақ **Лицензиялық кілттерді пайдалану туралы есеп** жасап, қарауға да болады.

Нәтижелер

Сценарий аяқталғаннан кейін, сіз өз ұйымыңыздың желісін қорғау туралы хабардар боласыз және осылайша, одан әрі қорғау үшін әрекеттерді жоспарлай аласыз.

Басқару консолінде түс индикаторлары мен тіркелген оқиғаларды мониторингтеу

Басқару консолінде Kaspersky Security Center және басқарылатын құрылғылардың ағымдағы күйін түс индикаторлары арқылы жылдам бағалауға болады. Индикаторлар **Мониторинг** қойыншасындағы **Басқару сервері** торабының жұмыс аймағында көрсетіледі. Қойыншада түсті индикаторларға және тіркелген оқиғаларға ие алты ақпараттық блок бар. Түсті индикатор – панельдің сол жағындағы түсті тік жолақ. Индикаторы бар әрбір блок Kaspersky Security Center жеке функционалды аймағына жауап береді (төмендегі кестені қараңыз).

Басқару консоліндегі түсті индикаторлардың жауапкершілік аймақтары

Панель атауы	Түсті индикатордың жауапкершілік аймағы
Орналастыру	Ұйым желісіндегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнату.
Басқару схемасы	Басқару тобы құрылымы. Желіні сканерлеу. Құрылғыны жылжыту ережелері
Қорғаныс параметрлері	Қауіпсіздік бағдарламасының функциялары: қорғаныс күйі, зиянды БҚ іздеу.
Жаңарту	Жаңартулар және патчтар.
Мониторинг	Қорғаныс күйі
Басқару сервері	Басқару сервері функциялары мен сипаттары.

Индикаторда бес түстің бірі болуы мүмкін (төмендегі кестені қараңыз). Индикатордың түсі Kaspersky Security Center ағымдағы күйіне және тіркелген оқиғаларға байланысты.

Индикаторлардың түсті кодтамалары

Күй	Индикатор түсі	Индикатор түсінің мәні
Ақпараттық	Жасыл	Әкімшінің араласуы қажет емес.
Ескерту	Сары	Әкімшінің араласуы қажет.
Критикалық	Қызыл	Күрделі мәселелер бар. Оларды шешу үшін әкімшінің араласуы қажет.
Ақпараттық	Көгілдір	Басқарылатын құрылғылардың қауіпсіздігіне қауіп төндірмейтін оқиғалар тіркелді.
Ақпараттық	Сұр	Оқиға туралы ақпарат жоқ немесе әлі алынған жоқ.

Әкімші мақсаты – индикаторларды **Мониторинг** қойыншасының барлық ақпараттық тақталарында "жасыл" күйінде қолдау.

Ақпараттық тақталарда түс индикаторлары мен Kaspersky Security Center күйіне әсер ететін тіркелген оқиғалар да көрсетіледі (төмендегі кестені қараңыз).

Тіркелген оқиғалар индикаторының атауы, сипаттамасы және түсі

Индикатор түсі	Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Сипаттамасы
Қызыл	**%1 құрылғыда лицензияның жарамдылық мерзімі бітті**	IDS_AK_STATUS_LIC_EXPAIRED	Бұл түрдегі оқиғалар коммерциялық лицензияның мерзімі өткен кезде орын алады. Күніне бір рет Kaspersky Security Center бағдарламасы лицензияның лицензия мерзімінің өтпегенін тексеріп тұрады. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, Kaspersky Security Center қолданбасы Базалық функционалдылық режимінде жұмыс істейді. Kaspersky Security Center бағдарламасын пайдалануды жалғастыру үшін коммерциялық лицензияның жарамдылық мерзімін ұзартыңыз.
Қызыл	**Қауіпсіздік бағдарламасы іске қосылмаған құрылғылардың саны: %1 құрылғы**	IDS_AK_STATUS_AV_NOT_RUNNING	Бұл түрдегі оқиғалар құрылғыда орнатылған қауіпсіздік бағдарламасы жұмыс істемей тұрғанда орын алады. Құрылғыда Kaspersky Endpoint Security бағдарламасы жұмыс істеп тұрғанын тексеріңіз.
Қызыл	**Қорғаныс өшірілген құрылғылардың саны: %1 құрылғы**	IDS_AK_STATUS_RTP_NOT_RUNNING	Бұл түрдегі оқиғалар құрылғыдағы қорғаныс бағдарламасы белгіленген уақыттан артық өшірілген кезде орын алады. Құрылғыдағы ағымдағы нақты уақыт режимінде қорғау күйін тексеріңіз және сізге қажет барлық қорғаныс құрамдастары қосылғанына көз жеткізіңіз.

Индикатор түсі	Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Сипаттамасы
Қызыл	**Құрылғылардағы бағдарламалық жасақтамада осалдық анықталды**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Осы түрдегі оқиғалар *осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыда орнатылған бағдарламаларда көрсетілген критикалық деңгейі бар осалдықтарды анықтаған кезде орын алады. Бағдарламаларды басқару қалтасының **Бағдарламалық жасақтама жаңартулары** ішкі қалтасында **қолжетімді жаңартулар тізімін тексеріңіз**. Бұл қалтада Microsoft корпорациясының және құрылғыларға таратылуы мүмкін басқа бағдарламалық жасақтама өндірушілерінің Басқару сервері алған жаңартулардың тізімі бар. Қолжетімді жаңартулар туралы ақпаратты қараңыз және оларды құрылғыңызға орнатыңыз.
Қызыл	**Критикалық оқиғалар Басқару серверінде тіркелді**	IDS_AK_STATUS_EVENTS_OCCURED	Бұл түрдегі оқиғалар Басқару серверінің критикалық оқиғалары анықталған кезде орын алады. Басқару серверінде сақталған оқиғалар тізімін тексеріңіз, содан кейін критикалық оқиғаларды рет-ретімен түзетіңіз.
Қызыл	**Басқару серверінің оқиғаларынан қателер тіркелді**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Бұл түрдегі оқиғалар Басқару сервері жағында күтпеген қателер тіркелгенде орын алады. Басқару серверінде сақталған оқиғалар тізімін тексеріңіз, содан кейін критикалық оқиғаларды рет-ретімен түзетіңіз.
Қызыл	**%1 құрылғыға қосылым жоғалды**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Бұл түрдегі оқиғалар Басқару сервері мен құрылғы арасындағы қосылым жоғалған кезде орын алады. Ажыратылған құрылғылар тізімін қарап шығыңыз және оларды қайта қосып көріңіз.
Қызыл	**%1 құрылғы Басқару серверіне ұзақ уақыт бойы қосылмаған**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Осы түрдегі оқиғалар құрылғы Басқару серверіне белгіленген уақыттан артық қосылмаған кезде орын алады, себебі құрылғы өшірулі. Құрылғының қосулы екенін және Желілік агент жұмыс істеп тұрғанын тексеріңіз.
Қызыл	**%1 құрылғының күйі «Бәрі дұрыс» күйінен басқаша**	IDS_AK_STATUS_HOST_NOT_OK	Бұл түрдегі оқиғалар Басқару серверіне қосылған *OK* құрылғысының күйі *Критикалық* немесе *Ескерту* күйіне өзгерген кезде орын алады. Ақаулықты Kaspersky Security Center қашықтан диагностикалау утилитасын пайдаланып шешуге болады.
Қызыл	**Дерекқорлар ескірген құрылғылардың саны: %1 құрылғы**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Бұл түрдегі оқиғалар құрылғыдағы антивирустық дерекқорлар белгілі бір уақыт аралығында жаңартылмаған кезде орын алады. Kaspersky антивирустық дерекқорларын жаңарту үшін нұсқауларды орындаңыз.
Қызыл	**Windows Update жаңартуларын тексеру орындалмағанына көп болған құрылғы(лар)дың саны: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Осы түрдегі оқиғалар *Windows Update синхрондау* тапсырмасы көрсетілген уақыттан артық орындалмаған кезде орын алады. Windows Update жаңартуларын Басқару серверімен синхрондау үшін нұсқауларды орындаңыз.
Қызыл	**Kaspersky Security Center арналған %1 плагин орнатылуы тиіс**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Бұл түрдегі оқиғалар Kaspersky бағдарламалары үшін қосымша плагиндерді орнату қажет болғанда орын алады. Kaspersky техникалық қолдау қызметінің веб-сайтынан Kaspersky бағдарламасы үшін қажетті басқару плагиндерін жүктеп алыңыз және орнатыңыз.

Есептер, статистика және хабарландырулармен жұмыс

Бұл бөлімде Kaspersky Security Center бағдарламасындағы есептермен, статистикамен, сондай-ақ оқиғалар мен құрылғылардың таңдауымен жұмыс істеу туралы және Басқару серверінің хабарландыру параметрлерін конфигурациялау туралы ақпарат берілген.

Есептермен жұмыс

Kaspersky Security Center-дегі есептер басқарылатын құрылғылардың күйі туралы ақпаратты қамтиды. Есептер Басқару серверінде сақталған ақпарат негізінде құрылады. Сіз келесі нысандар үшін есептер жасай аласыз:

- белгілі бір параметрлер бойынша жасалған құрылғылардың таңдаулары үшін;
- басқару топтары үшін;
- әртүрлі басқару топтарындағы құрылғылар жиынтығы үшін;
- желідегі барлық құрылғылар үшін (орналастыру есебінде).

Бағдарламада стандартты есеп шаблондарының жиынтығы бар. Сондай-ақ, пайдаланушы есеп үлгілерін жасау мүмкіндігі бар. Есептер **Басқару сервері** консолі ағашының қалтасындағы Бағдарламаның негізгі терезесінде көрсетіледі.

Есеп үлгісін жасау

Есеп үлгісін жасау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. **Жаңа есеп үлгісі** түймесін басыңыз.

   Нәтижесінде, есеп үлгісін жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысы аяқталғаннан кейін, құрастырылған есеп үлгісі консоль ағашының **Басқару сервері** таңдалған қалтасының құрамына қосылады. Бұл үлгіні есептерді құрастыру және қарау үшін пайдалануға болады.

Есеп үлгісінің сипаттарын қарау және өзгерту

Есеп үлгісінің негізгі сипаттарын, мысалы, есеп үлгісінің атауын немесе есепте көрсетілетін өрістерді қарауға және өзгертуге болады.

Есеп үлгісінің сипаттарын қарау және өзгерту үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. Есеп үлгілері тізімінен қажетті есеп үлгісін таңдаңыз.
4. Таңдалған есеп үлгісінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   Балама ретінде, алдымен есепті құрастырып, кейін **Есеп үлгісінің сипаттарын ашу** немесе **Есеп бағандарын конфигурациялау** түймесін басуға болады.
5. Ашылған терезеде есеп үлгісінің сипаттарын өзгертуге болады. Әрбір есептің сипаттарында тек төменде сипатталған бөлімдердің кейбірі ғана болуы мүмкін.

   - **Жалпы** бөлімі:
     - Есеп үлгісінің атауы
     - **Көрсетілетін жазбалардың ең көп саны**

       Егер бұл параметр қосылса, есептің егжей-тегжейлі деректері бар кестеде көрсетілетін жазбалар саны көрсетілген мәннен аспайды.

       Есеп жазбалары алдымен есеп үлгісі сипаттарының **Өрістер** → **Мәліметтер өрістері** бөлімінде көрсетілген ережелерге сай сұрыпталады, содан соң қорытқы жазбалардың бірінші бөлігі ғана сақталады. Есептің егжей-тегжейлі деректері бар кесте тақырыбында, көрсетілетін жазбалар саны және есеп үлгісінің басқа параметрлеріне сәйкес келетін жазбалардың жалпы саны көрсетілген.

       Егер бұл параметр өшірулі болса, есептің егжей-тегжейлі деректері бар кестеде барлық жазбалар көрсетіледі. Бұл параметрді өшіру ұсынылмайды. Көрсетілетін есеп жазбаларының санын шектеу дерекқорды басқару жүйесіне түсетін жүктемені және есепті қалыптастыру мен экспорттауға кететін уақытты азайтады. Кейбір есептерде тым көп жазбалар бар. Мұндай жағдайларда барлық жазбаларды қарау және талдау тым көп еңбекті қажет етуі мүмкін. Сондай-ақ мұндай есепті жасау кезінде құрылғыңыздың жады таусылуы мүмкін, демек есепті көре алмайсыз.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша, 1000 мәні көрсетілген.
     - **Басып шығаруға арналған нұсқа**

       Есеп басып шығару үшін оңтайландырылған: көрнекі қолжетімділік үшін кейбір мәндер арасында бос орындар қосылды.

       Әдепкі бойынша, параметр қосулы.
   - **Өрістер** бөлімі.

     Есепте көрсетілетін өрістерді және осы өрістердің ретін таңдап, есептегі ақпарат өрістердің әрқайсысы бойынша сұрыпталуы және сүзілуі қажеттігін конфигурациялаңыз.
   - **Уақыт аралығы** бөлімі.

     Есеп мерзімін өзгертіңіз. Қолжетімді мәндері:
     - екі көрсетілген күн арасында;
     - көрсетілген күннен есеп жасалған күнге дейін;
     - есеп жасалған күннен бастап, минус көрсетілген күндер саны, есеп жасалған күнге дейін.

- **Топ**, **Құрылғыны таңдау**, немесе **Құрылғылар** бөлімдері.

  Есеп жасалатын клиент құрылғылары жиынтығын өзгертіңіз. Үлгіні жасау кезінде көрсетілген параметрлерге байланысты, осы бөлімдердің біреуі ғана болуы мүмкін.

- **Параметрлер** бөлімі.

  Есеп параметрлерін өзгертіңіз. Параметрлер жиынтығы нақты есепке байланысты.

- **Қауіпсіздік** бөлімі. **Басқару серверінен параметрлерді иелену**

  Егер бұл параметр қосулы болса, есеп параметрлері Басқару серверінен иеленеді.

  Бұл параметр өшірулі болса, сіз есеп параметрлерін конфигурациялай аласыз. Сіз пайдаланушыға немесе пайдаланушылар тобына рөл тағайындай аласыз немесе есепке қатысты тұрғыда пайдаланушыға немесе пайдаланушылар тобына құқықтар тағайындай аласыз.

  Әдепкі бойынша, параметр қосулы.

  > **Қауіпсіздік** бөлімі, интерфейс параметрлері терезесінде **Қауіпсіздік параметрлері бар тарауларды көрсету** жалаушасы қойылса қолжетімді болады.

- **Басқару серверлерінің иерархиясы** бөлімі:

  - **Қосалқы және виртуалды Басқару серверлерінен алынған деректерді қамту**

    Бұл параметр өшірулі болса, есеп есеп үлгісі жасалған Басқару серверіне бағынатын қосалқы және виртуалды Басқару серверлерінен алынған ақпаратты қамтиды.

    Тек ағымдағы Басқару серверінің деректерін ғана қарағыңыз келсе, осы параметрді өшіріңіз.

    Әдепкі бойынша, параметр қосулы.

  - **Кірістіру деңгейіне дейін**

    Есепте, ағымдағы Басқару серверінің астында, көрсетілген мәннен төмен немесе оған тең тіркеме деңгейінде орналасқан қосалқы және виртуалды Басқару серверлерінің деректері бар.

    Әдепкі бойынша, 1 мәні көрсетілген. Егер сіз есепте ағаштың ең төменгі деңгейінде орналасқан қосалқы Басқару серверлері туралы ақпаратты көргіңіз келсе, бұл мәнді өзгерте аласыз.

  - **Деректерді күту уақыт аралығы (мин)**

    Есеп үлгісі жасалған Басқару сервері есепті жасау үшін көрсетілген уақыт ішінде қосалқы Басқару серверлерінен деректерді күтеді. Егер деректер көрсетілген уақыт аралығында қосалқы Басқару серверінен алынбаса, есеп кез келген жағдайда іске қосылады. Нақты деректердің орнына есепте кэштен алынған деректер көрсетіледі (**бағынышты басқару серверлерінен деректерді кэштеу** опциясы қосылған болса) немесе басқа жағдайда **қолжетімсіз** болады.

    Әдепкі бойынша күту уақыты – 5 минут.

  - **Қосалқы Басқару серверлерінен алынған деректерді кэштеу**

    Қосалқы Басқару серверлері деректерді үнемі есеп үлгісі жасалған негізгі Басқару серверіне жібереді. Берілген деректер кэште сақталады.

    Басқару сервері есепті құру кезінде қосалқы Басқару серверінің деректерін ала алмаса, есеп кэштегі деректерді көрсетеді. Бұл жағдайда, деректер кэшке жіберілген күн көрсетіледі.

    Бұл параметрді қосу арқасында өзекті деректерді алу мүмкін болмаса да, қосалқы Басқару серверлерінен алынған ақпаратты көруге мүмкіндік беріледі. Алайда, көрсетілетін деректер ескірген болуы мүмкін.

    Әдепкі бойынша, параметр өшірулі.

- **Кэшті жаңарту жиілігі (сағ)**

  Қосалқы Басқару серверлері деректерді үнемі есеп үлгісі жасалған негізгі Басқару серверіне жібереді. Сіз осы кезеңді сағат түрінде көрсете аласыз. Егер 0 мәні белгіленсе, деректер тек есеп шығару кезінде беріледі.

  Әдепкі бойынша, 0 мәні көрсетілген.

- **Қосалқы Басқару серверлерінен толық ақпаратты жіберу**

  Жасалған есепте егжей-тегжейлі деректер кестесі есеп үлгісі жасалған негізгі Басқару серверінің қосалқы Басқару серверлерінен алынған ақпаратты қамтиды.

  Егер бұл параметр қосылса, онда есепті құру баяулайды және Басқару серверлері арасындағы трафик артады. Дегенмен, сіз барлық деректерді бір есепте көре аласыз.

  Бұл параметрді қоспау үшін сіз ақаулы қосалқы Басқару серверін табу үшін есеп деректерін талдай аласыз, содан кейін бірдей есепті тек сол ақаулы Басқару сервері үшін жасай аласыз.

  Әдепкі бойынша, параметр өшірулі.

Есеп үлгілеріндегі кеңейтілген сүзгі пішімі

Kaspersky Security Center 15.1 бағдарламасында есеп үлгілеріне кеңейтілген сүзгі пішімін қолдана аласыз. Кеңейтілген сүзгі пішімі әдепкі бойынша пішіммен салыстырғанда үлкен икемділікті қамтамасыз етеді. Төменде көрсетілгендей есепті жасау кезінде OR логикалық операторы арқылы есепке қолданылатын сүзгілер жиынтығын пайдаланып, күрделі сүзу шарттарын жасауға болады:

Сүзгі[1](Өріс[1] AND Өріс[2]... AND Өріс[n]) OR Сүзгі[2](Өріс[1] AND Өріс[2]... AND Өріс[n]) OR... Сүзгі[n](Өріс[1] AND Өріс[2]... AND Өріс[n])

Бұдан бөлек, кеңейтілген сүзгі пішімі көмегімен сіз сүзгінің белгілі бір өрістері үшін салыстырмалы уақыт пішімінде уақыт аралығының мәнін белгілей аласыз (мысалы, "Соңғы N күн ішінде" шарты арқылы). Уақыт аралығы шарттарының қолжетімді болуы және жиынтығы есеп үлгісінің түріне байланысты.

Сүзгіні кеңейтілген пішімге түрлендіру

Есеп үлгілері үшін кеңейтілген сүзгі пішіміне Kaspersky Security Center 12 және одан да жоғары нұсқасында ғана қолдау көрсетіледі. Сүзгіні әдепкі бойынша кеңейтілген пішімге түрлендіргеннен кейін, есеп үлгісі Kaspersky Security Center бағдарламасының бұрығы нұсқалары орнатылған желіңіздегі Басқару серверлерімен үйлесімді болмай қалады. Осы Басқару серверлерінен алынатын ақпарат есеп үшін алынбайды.

Әдепкі пішімнен кеңейтілген пішімге түрлендіру үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. Есеп үлгілері тізімінен қажетті есеп үлгісін таңдаңыз.
4. Таңдалған есеп үлгісінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
5. Көрсетілген сипаттар терезесінен **Өрістер** бөлімін таңдаңыз.
6. **Мәліметтер өрістері** қойындысында **Сүзгіні түрлендіру** сілтемесінен өтіңіз.

7. Пайда болған терезеде **OK** түймесін басыңыз.

> Кеңейтілген сүзгі пішіміне түрлендіру, ол қолданылатын есеп үлгісі үшін қайтымсыз болып саналады. **Сүзгіні түрлендіру** сілтемесінен кездейсоқ өткен болсаңыз, есеп үлгісі сипаттары терезесінде **Бас тарту** түймесін басып, өзгерістердің күшін жоя аласыз.

8. Өзгерістерді қолдану үшін, **OK** түймесін басып, есеп үлгісі сипаттары терезесін жабыңыз.

   Есеп үлгісі сипаттары терезесі қайта ашылған кезде, жаңа қолжетімді **Сүзгілер** бөлімі көрсетіледі. Бұл бөлімде кеңейтілген сүзгі пішімін конфигурациялай аласыз.

Кеңейтілген сүзгіні конфигурациялау

Есеп үлгісінде кеңейтілген сүзгі параметрлерін конфигурациялау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. Есеп үлгілері тізімінде, бұған дейін кеңейтілген сүзгі пішіміне түрлендірілген есеп үлгісін таңдаңыз.
4. Таңдалған есеп үлгісінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
5. Көрсетілген сипаттар терезесінен **Сүзгілер** бөлімін таңдаңыз.

   Есеп үлгісі кеңейтілген сүзгі пішіміне түрлендірілмеген болса, онда **Сүзгілер** бөлімі көрсетілмейді.

   Есеп үлгісі сипаттары терезесінде, **Сүзгілер** бөлімінде есепке қолданылған сүзгілер тізімін қарап, өзгерте аласыз. Тізімдегі әрбір сүзгі бірегей атауға ие және есептегі тиісті өрістерге арналған сүзгілер жиынтығы болып саналады.
6. Сүзгі сипаттары терезесін келесі тәсілдердің бірімен ашыңыз:
   - Сүзгіні жасау үшін, **Қосылуда** түймесін басыңыз.
   - Қолданыстағы сүзгіні өзгерту үшін, қажетті сүзгіні таңдап, **Өзгерту** түймесін басыңыз.
7. Ашылған терезеде сүзгінің міндетті өрістерінің мәндерін таңдап, көрсетіңіз.
8. Өзгерістерді сақтау және терезені жабу үшін **OK** түймесін басыңыз.

   Сүзгі жасап жатсаңыз, **OK** түймесін баспас бұрын, сүзгінің атауы **Сүзгі атауы** өрісінде көрсетілуі тиіс.
9. **OK** түймесін басып, есеп үлгісі сипаттары терезесін жабыңыз.

   Есеп үлгісіндегі кеңейтілген сүзгі конфигурацияланған. Енді сіз осы есеп үлгісін қолдана отырып, есептерді жасай аласыз.

Есепті жасау және қарау

Есепті жасау және қарау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.

3. Тінтуірді екі рет басу арқылы үлгілер тізімінен өзіңізді қызықтыратын есеп үлгісін таңдаңыз.

   Таңдалған есеп үлгісі көрсетіледі.

Есепте келесі деректер көрсетіледі:

- Есептің түрі мен атауы, оның қысқаша сипаттамасы мен есепті кезеңі және есептің қай құрылғылар тобы үшін жасалғаны туралы ақпарат.
- Есептің анағұрлым тән деректері бар графикалық диаграмма.
- Есептелетін есеп көрсеткіштері бар жиынтық кесте.
- есептің мәліметтер өрістері бар кесте.

Есепті сақтау

Қалыптасқан есепті сақтау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. Үлгілер тізімінен сізді қызықтыратын есеп үлгісін таңдаңыз.
4. Таңдалған есеп үлгісінің контекстік мәзірінен **Сақтау** тармағын таңдаңыз.

   Нәтижесінде, есепті сақтау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысы аяқталғаннан кейін, есеп файлы сақталған қалта ашылады.

Есепті XLS файлы ретінде сақтаған кезде, логотип және датаграмма сияқты барлық байланысты кескіндер бөлек файлдар ретінде сақталады.

Есептерді жеткізу тапсырмасын жасау

Есептерді электрондық пошта арқылы таратуға болады. Есептерді Kaspersky Security Center-ге жіберу есепті тарату тапсырмасы арқылы жүзеге асырылады.

Бір есепті жеткізу тапсырмасын жасау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. Үлгілер тізімінен сізді қызықтыратын есеп үлгісін таңдаңыз.
4. Таңдалған есеп үлгісінің контекстік мәзірінен **Есептерді жеткізу** тармағын таңдаңыз.

   Нәтижесінде, таңдалған есепті жіберу тапсырмаларын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Бірнеше есепті жеткізу тапсырмасын жасау үшін:

1. Өзіңізге қажетті Басқару сервері атауы бар түйіндегі консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Тапсырмалар** қалтасының жұмыс аймағындағы **Тапсырма жасау** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   Жасалған есеп жеткізу тапсырмасы консоль ағашының **Тапсырмалар** қалтасында көрсетіледі.

Kaspersky Security Center орнату кезінде электрондық пошта параметрлері белгіленген жағдайда, есепті жеткізу тапсырмасы автоматты түрде жасалады.

1-қадам. Тапсырма түрін таңдау

Тапсырма түрін таңдау терезесінде тапсырма тізімінде **Есептерді жеткізу** тапсырма түрін таңдаңыз.

Келесі қадамға өту үшін **Келесі** түймесін басыңыз.

2-қадам. Есеп түрін таңдау

Есеп түрін таңдау терезесінде тапсырма жасауға арналған шаблондар тізімінде есеп түрін таңдаңыз.

Келесі қадамға өту үшін **Келесі** түймесін басыңыз.

3-қадам. Есеппен жасалатын әрекеттер

Есептерге қолданылатын әрекет бөлімінде келесі параметрлерді көрсетіңіз:

- **Электрондық пошта арқылы есептер жіберу**

  Егер бұл параметр қосылса, бағдарлама қалыптасқан есептерді электрондық пошта арқылы жібереді.

  Есепті электрондық пошта арқылы жіберу параметрлерін **Электрондық пошта арқылы хабарландыру параметрлері** сілтемесі арқылы конфигурациялауға болады. Параметр қосулы болса, сілтеме қолжетімді болады.

  Егер бұл параметр өшірулі болса, бағдарлама есептерді сақтау үшін есептерді көрсетілген қалтаға сақтайды.

  Әдепкі бойынша, параметр өшірулі.

- **Есептерді ортақ қалтада сақтау**

  Егер бұл параметр қосылса, бағдарлама есептерді жалаушаның астындағы өрісте көрсетілген қалтаға сақтайды. Есептерді ортақ қатынасы бар қалтаға сақтау үшін осы қалтаға UNC жолын көрсетіңіз. Бұл жағдайда, **Тапсырманы іске қосу үшін есептік жазбаны таңдау** терезесінде осы қалтаға қатынасу үшін пайдаланушы есептік жазбасы мен құпиясөзін белгілеу керек.

  Егер бұл параметр өшірулі болса, бағдарлама есептерді қалтаға сақтамайды, оларды электрондық пошта арқылы жібереді.

  Әдепкі бойынша, параметр өшірулі.

- **Бір түрдегі бұрынғы есептердің үстінен жазу**

  Егер бұл параметр қосулы болса, тапсырманы іске қосқан сайын жаңа есеп файлы есептерді сақтау қалтасында тапсырманы алдыңғы іске қосқан кезде сақталған файлды алмастырады.

  Егер бұл параметр өшірулі болса, есеп файлдары қайта жазылмайды. Тапсырманы іске қосқан сайын қалтада жеке есеп файлы сақталады.

Есепті қалтада сақтау жалаушасы қойылса, жалауша қолжетімді.

Әдепкі бойынша, параметр өшірулі.

- **Ортақ қалтаға қатынасу үшін есептік жазбаны белгілеу**

  Егер бұл параметр қосылса, есеп қалтаға жазылатын есептік жазбаны көрсетуге болады. **Есептерге қолданылатын әрекет** терезесінде **Қалтада есепті сақтау** параметрі ретінде ортақ қатынасы бар қалтаға UNC жолы көрсетілсе, осы қалтаға қатынасу үшін есептік жазба мен құпиясөзді көрсету керек.

  Егер бұл параметр өшірулі болса, есеп Басқару сервері есептік жазбасы атынан қалтаға жазылады.

  Есепті қалтада сақтау жалаушасы қойылса, жалауша қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

Есепті XLS файлы ретінде сақтаған немесе жіберген кезде, логотип және датаграмма сияқты барлық байланысты кескіндер бөлек файлдар ретінде сақталады.

Келесі қадамға өту үшін **Келесі** түймесін басыңыз.

4-қадам. Тапсырманы іске қосу үшін есептік жазбаны таңдау

Тапсырманы іске қосу үшін есептік жазбаны таңдау терезесінде тапсырманы қандай есептік жазбамен іске қосу керектігін көрсетуге болады. Келесі нұсқалардың бірін таңдаңыз:

- **Әдепкі есептік жазба**

  Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Есептік жазбаны көрсету**

  Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

  - **Есептік жазба**

    Тапсырманы іске қосатын есептік жазба.

  - **Құпиясөз**

    Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

Келесі қадамға өту үшін **Келесі** түймесін басыңыз.

5-қадам. Тапсырма кестесін конфигурациялау

Тапсырма кестесін конфигурациялау терезесінде тапсырманы бастау кестесін құрастыруға болады. Қажет болса, келесі параметрлерді белгілеңіз:

- **Кесте бойынша іске қосу:**

  Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

  - **N сағат сайын**

    Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

- **N күн сайын**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N апта сайын**

  Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

  Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

  Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Апта сайын**

  Тапсырма апта сайын, көрсетілген күні және көрсетілген уақытта іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

> Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

6-қадам. Тапсырманың атауын анықтау

Тапсырма атауын анықтау терезесінде жасалатын ереженің атауын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды (`"*<>?\:|`) қамтуы мүмкін емес.

Келесі қадамға өту үшін **Келесі** түймесін басыңыз.

7-қадам. Тапсырманы жасауды аяқтау

Тапсырманы жасауды аяқтау терезесінде шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылуын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** жалаушасын қойыңыз.

Статистикалық ақпаратпен жұмыс

Қорғаныс жүйесінің және басқарылатын құрылғылардың күйі туралы статистикалық ақпарат конфигурацияланатын ақпараттық тақталар түрінде көрсетіледі. Статистикалық ақпарат **Статистика** қойыншасындағы **Басқару сервері** торабының жұмыс аймағында көрсетіледі. Бұл қойынша екінші деңгейлі бірнеше қойыншаны да қамтиды (беттер). Әрбір бетте статистикалық ақпараты бар ақпараттық тақталар, сондай-ақ корпоративтік жаңалықтарға және Kaspersky басқа материалдарына сілтемелер көрсетіледі. Статистикалық ақпарат ақпараттық тақталарда дөңгелек немесе бағандық диаграммалар не кестелер түрінде көрсетілген. Ақпараттық тақталардағы деректер бағдарламаның жұмыс істеуі процесінде жаңартылады және қауіпсіздік бағдарламасының ағымдағы күйін көрсетеді.

Статистика қойыншасындағы екінші деңгейлі қойыншалар жинағын, қойыншасы бар әрбір беттегі ақпараттық тақталар жинағын, сондай-ақ ақпараттық тақталарда деректерді көрсету тәсілін де өзгертуге болады.

Статистика қойыншасындағы ақпараттық тақталармен бірге екінші деңгейлі жаңа қойыншаны қосу үшін:

1. **Статистика** қойыншасының жоғарғы оң жақ бұрышындағы **Көріністі реттеу** түймесін басыңыз.

   Нәтижесінде, статистика сипаттары терезесі ашылады. Терезеде, қазіргі уақытта **Статистика** қойыншасында қамтылған қойыншалары бар беттер тізімі келтірілген. Терезеде қойыншадағы беттерді көрсету тәртібін өзгертуге, беттерді қосуға және жоюға, **Сипаттар** түймесі бойынша беттердің сипаттарын конфигурациялауға өтуге болады.

2. **Қосу** түймесін басыңыз.

   Жаңа бет сипаттары терезесі ашылады.

3. Жаңа бетті конфигурациялаңыз:

   - **Жалпы** бөлімінде беттің атауын көрсетіңіз.
   - **Ақпараттық тақталар** бөлімінде **Қосу** түймесі бойынша бетте көрсетілуі тиісті ақпараттық тақталарды қосыңыз.

     Сипаттар түймесі бойынша **Ақпараттық тақталар** бөлімінде қосылған ақпарат тақталарының сипаттарын реттеуге болады: диаграмма құрылатын тақтадағы диаграмманың атауы, типі және түрі.

4. **ОК** түймесін басыңыз.

Ақпараттық тақталары қамтылған қойыншалары бар қосылған бет **Статистика** қойыншасында көрсетіледі. Параметрлер (⚙) белгішесін басып, бірден бетті және бетте таңдалған ақпараттық тақтаны конфигурациялауға көшуге болады.

Оқиға хабарландырулары параметрлерін конфигурациялау

Kaspersky Security Center бағдарламасы клиент құрылғыларындағы оқиғалар туралы әкімшіге хабарлау тәсілін таңдауға және хабарландыру параметрлерін конфигурациялауға мүмкіндік береді:

- Электрондық пошта. Оқиға орын алған кезде, бағдарлама көрсетілген электрондық пошта мекенжайларына хабарландыру жібереді. Хабарландыру хабарын конфигурациялай аласыз.
- SMS. Оқиға орын алған кезде, бағдарлама көрсетілген телефон нөмірлеріне хабарландырулар жібереді. Пошта шлюзі арқылы SMS хабарландыруларын жіберуді конфигурациялауға болады.
- Орындалатын файл. Құрылғыда оқиға болған кезде орындалатын файл әкімшінің жұмыс станциясында іске қосылады. Орындалатын файлдың көмегімен әкімші болған оқиғаның параметрлерін ала алады.

Клиент құрылғыларындағы оқиғалар туралы хабарландыру параметрлерін конфигурациялау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. **Хабарландырулар мен оқиғаларды экспорттау параметрлерін конфигурациялау** сілтемесі арқылы өтіп, ашылатын тізімнен **Хабарландыруларды конфигурациялау** мәнін таңдаңыз.

   Сипаттар: Оқиғалар терезесі ашылады.

4. **Хабарландыру** бөлімінде хабарландыру тәсілін таңдаңыз (электрондық пошта, SMS, іске қосылатын орындалатын файл) және хабарландыру параметрлерін конфигурациялаңыз:

   - **Электрондық пошта**

     Электрондық пошта қойындысы оқиғаларға арналған электрондық хат хабарландыруларын конфигурациялауға мүмкіндік береді.

     Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады.

     SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

     - IPv4 мекенжайы немесе IPv6 мекенжайы;
     - Windows желісіндегі құрылғының атауы (NetBIOS атауы);
     - SMTP сервері DNS атауы.

     SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

     DNS MX іздеуін пайдалану параметрін қоссаңыз, SMTP серверінің бірдей DNS атауы үшін IP мекенжайының бірнеше MX жазбасын қолдана аласыз. Бір DNS атауында, алынған электрондық пошталардың әртүрлі басымдықтары бар бірнеше MX жазбалары болуы мүмкін. Басқару сервері MX жазбаларының басымдылығының өсуі ретімен SMTP серверіне электрондық пошта бойынша хабарландырулар жіберуге тырысады. Әдепкі бойынша, параметр өшірулі.

     > **DNS MX іздеуін пайдалану** параметрін қосып, TLS параметрін қолдануға рұқсат бермесеңіз, онда хабарландыруларды электрондық пошта бойынша жіберу кезінде қосымша қорғаныс шарасы ретінде сіздің серверлік құрылғыңызда DNSSEC параметрлерін қолдану ұсынылады.

     Қосымша параметрлерді белгілеу үшін **Параметрлер** сілтемесінен өтіңіз:

     - Тақырып (электрондық пошта тақырыбының атауы).
     - Электрондық пошта жіберушінің мекенжайы.
     - ESMTP аутентификациясы параметрлері.

     SMTP сервері үшін ESMTP аутентификациясы параметрі қосылған болса, SMTP серверінде түпнұсқалық растама үшін есептік жазбаны көрсету керек.

     - SMTP сервері үшін TLS параметрлері:
       - **TLS қолданбау**

         Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

       - **SMTP сервері қолдаса, TLS қолдану**

         SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

       - **Әрқашан TLS пайдалану, Сервер сертификатының жарамдылық мерзімін тексеру**

         TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

Әрқашан TLS пайдалану, Сервер сертификатының жарамдылық мерзімін тексеру үшін мәнін қолдануды ұйғарсаңыз, сіз SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

SMTP сервері үшін TLS параметрлерін көрсетуіңізге болады:

- SMTP серверінің сертификаты файлын таңдаңыз:

Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

- Клиент сертификаты файлын таңдаңыз:

Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

- X.509 сертификаты:

Сертификаты бар файлды және жеке кілт файлын көрсетуіңіз қажет. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- pkcs12 контейнері:

Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

Хабарландыру хабары өрісінде, оқиға туындаған кезде бағдарлама жіберетін оқиға туралы хабарландырудың стандартты мәтіні қамтылған. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер бар. Хабар мәтінін, оқиғаның егжей-тегжейлі деректері бар жаңа алмастырылатын параметрлерді қосу арқылы өзгертуге болады. Алмастырылатын параметрлер тізімі өрістің оң жағындағы түймені басу арқылы қолжетімді.

Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Хабарлардың дұрыс конфигурацияланғанын тексеру үшін **Тексеру хабарын жіберу** түймесін басыңыз. Бағдарлама көрсетілген электрондық пошта мекенжайларына мәтіндік хабарлар жібереді.

- **SMS**

SMS қойыншасында ұялы телефонға түрлі оқиғалар туралы SMS хабарландыруларын жіберуді конфигурациялауға болады. SMS хабарлар пошта шлюзі арқылы жіберіледі.

Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады. Хабарландырулар, көрсетілген электрондық пошта мекенжайларымен байланысты нөмірлері бар телефондарға жеткізіледі.

SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

- IPv4 мекенжайы немесе IPv6 мекенжайы;
- Windows желісіндегі құрылғының атауы (NetBIOS атауы);
- SMTP сервері DNS атауы.

SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

Қосымша параметрлерді белгілеу үшін **Параметрлер** сілтемесінен өтіңіз:

- Тақырып (электрондық пошта тақырыбының атауы).
- Электрондық пошта жіберушінің мекенжайы.
- ESMTP аутентификациясы параметрлері.

Қажет болса, SMTP сервері үшін ESMTP аутентификациясы параметрі қосылған болса, SMTP серверінде түпнұсқалық растама үшін есептік жазбаны көрсетуге болады.

- SMTP сервері үшін TLS параметрлері

SMTP сервері осы протоколды қолдайтын болса, TLS қолдануды өшіре аласыз, TLS қолдана аласыз немесе тек TLS-ті күштеп қолдана аласыз. Егер сіз тек TLS пайдалануды ұйғарсаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, тек TLS пайдалануды ұйғарсаңыз, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификат көрсете аласыз.

- SMTP серверінің сертификаты файлын таңдаңыз

Сертификаттар тізімі бар файлды сенімді сертификаттау орталығынан (CA) ала аласыз және оны Kaspersky Security Center бағдарламасына жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт кодталмаған болса, құпиясөзде бос мән болуы мүмкін. **Хабарландыру хабары** өрісінде оқиға орын алған кезде қолданба жіберетін оқиға туралы ақпараты бар стандартты мәтін болады. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер бар. Хабар мәтінін, оқиғаның егжей-тегжейлі деректері бар жаңа алмастырылатын параметрлерді қосу арқылы өзгертуге болады. Алмастырылатын параметрлер тізімі өрістің оң жағындағы түймені басу арқылы қолжетімді.

Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Тексеру хабарын жіберу түймесі арқылы хабарландырулардың дұрыс конфигурацияланғанын тексеріңіз. Бағдарлама көрсетілген алушыларға мәтіндік хабарлар жібереді.

- **Іске қосылатын орындалатын файл**

Егер бұл хабарландыру тәсілі таңдалса, енгізу өрісінде оқиға болған кезде қандай бағдарлама іске қосылатынын көрсетуге болады.

Хабарландырулар санының шегін конфигурациялау сілтемесінен өту кезінде, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Сынақ хабарын жіберу түймесін басу арқылы, хабарлардың дұрыс конфигурацияланғанын тексеруге болады: бағдарлама көрсетілген электрондық пошта мекенжайларына мәтіндік хабарлар жібереді.

5. **Хабарландыру хабары** өрісінде оқиға болған кезде бағдарлама жіберетін мәтінді енгізіңіз.

   Мәтін өрісінің оң жағында орналасқан ашылмалы тізімнен хабарға оқиғаның егжей-тегжейі бар алмастырылатын параметрлерді қосуға болады (мысалы, оқиғаның сипаттамасы, пайда болу уақыты және т.б.).

   Хабарландыру мәтінінде % белгішесі болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

6. **Тексеру хабарын жіберу** түймесі арқылы хабарландырулардың дұрыс конфигурацияланғанын тексеріңіз.

   Бағдарлама көрсетілген алушыға сынақ хабарын жібереді.

7. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

Нәтижесінде, конфигурацияланған хабарландыру параметрлері клиент құрылғыларында болып жатқан барлық оқиғаларға таралады.

Оқиғаларды конфигурациялау бөлімінде, Басқару сервері параметрлерінде, саясат параметрлерінде немесе бағдарлама параметрлерінде белгіленген оқиғалар үшін хабарландыру параметрлерінің мәндерін өзгертуге болады.

SMTP сервері үшін сертификат жасау

SMTP сервері үшін сертификат жасау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар тораптыны таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. **Хабарландырулар мен оқиғаларды экспорттау параметрлерін конфигурациялау** сілтемесі арқылы өтіп, ашылатын тізімнен **Хабарландыруларды конфигурациялау** мәнін таңдаңыз.

   Оқиғалар сипаттары терезесі ашылады.

4. **Параметрлер** сілтемесі бойынша **Электрондық пошта** қойыншасында **Параметрлер** терезесін ашыңыз.
5. **Сертификатты көрсету** сілтемесі бойынша **Параметрлер** терезесінде **Қол қоюға арналған сертификат** терезесін ашыңыз.
6. **Қол қоюға арналған сертификат** терезесінде **Шолу** түймесін басыңыз.

   Сертификат терезесі ашылады.

7. **Сертификат түрі** ашылатын тізімінде сертификаттың жалпыға ортақ немесе жеке түрін таңдаңыз:

   - Жеке типтегі сертификат (**PKCS #12 контейнері**) таңдалған болса, сертификат файлы мен құпиясөзді көрсетіңіз.

   - Жалпыға ортақ сертификат (**X.509 сертификаты**) таңдалған болса:

     a. жеке кілт файлын (prk немесе pem кеңейтімі бар файл) көрсетіңіз;

     b. жеке кілт құпиясөзін көрсетіңіз;

     c. жалпыға ортақ кілт файлын (cer кеңейтімі бар файл) көрсетіңіз.

8. **ОК** түймесін басыңыз.

Нәтижесінде, SMTP сервері үшін сертификат жазып беріледі.

Оқиғалар таңдау

Kaspersky Security Center және басқарылатын бағдарламалар жұмысындағы оқиғалар туралы ақпарат Басқару сервері дерекқорында да, Microsoft Windows жүйелік журналында да сақталады. **Басқару сервері** түйінінің жұмыс аймағындағы Басқару сервері дерекқорынан ақпаратты **Оқиғалар** қойыншасында көре аласыз.

Оқиғалар қойыншасындағы ақпарат оқиғаларды таңдау тізімі түрінде көрсетілген. Әрбір таңдау тек белгілі бір түрдегі оқиғаларды қамтиды. Мысалы, "Құрылғы күйі – Критикалық" таңдауы тек құрылғы күйінің "Критикалық" күйіне өзгергені туралы жазбаларды қамтиды. Бағдарламаны орнатқаннан кейін **Оқиғалар** қойыншасында бірқатар стандартты оқиғалар таңдаулары болады. Сіз оқиғалардың қосымша (пайдаланушы) таңдауларын жасай аласыз, сонымен қатар оқиғалар туралы ақпаратты файлға экспорттай аласыз.

Оқиғалар таңдауын қарап шығу

Оқиғалар таңдауын қарап шығу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.

2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.

3. **Оқиғаларды таңдау** ашылмалы тізімінен өзіңізге қажетті оқиғалар таңдауын таңдаңыз.

   Осы таңдаудың оқиғалары жұмыс аймағында үнемі көрсетіліп тұруын қаласаңыз, таңдаудың жанындағы "Таңдаулы" (☆) белгішесін басыңыз.

Нәтижесінде, жұмыс аймағында Басқару серверінде сақталатын таңдалған түрдегі оқиғалар тізімі ұсынылады.

Оқиғалар тізіміндегі ақпаратты тізімнің кез келген бағанындағы деректердің өсуі немесе азаюы бойынша сұрыптауға болады.

Оқиғалар таңдау параметрлерін конфигурациялау

Оқиғалар таңдау параметрлерін конфигурациялау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. **Оқиғалар** қойыншасында қажетті оқиғалар таңдауын ашыңыз.
4. **Таңдау сипаттары** түймесін басыңыз.

Ашылған оқиға таңдау сипаттары терезесінде таңдау параметрлерін конфигурациялауға болады.

Оқиғалар таңдауын жасау

Оқиғалар таңдауын жасау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. **Таңдау жасау** түймесін басыңыз.
4. Ашылған **Жаңа оқиғаны таңдау** терезесінде жасалып жатқан таңдаудың атауын көрсетіп, **OK** түймесін басыңыз.

Нәтижесінде, **Оқиғаларды таңдау** ашылмалы тізімінде сіз көрсеткен атпен үлгі жасалады.

Әдепкі бойынша, жасалған оқиғалар таңдауы Басқару серверінде сақталатын барлық оқиғаларды қамтиды. Таңдауда тек сізді қызықтыратын оқиғалар көрсетілуі үшін таңдау параметрлерін конфигурациялау керек.

Оқиғалар таңдауын мәтіндік файлға экспорттау

Оқиғалар таңдауын мәтіндік файлға экспорттау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. **Импорттау/Экспорттау** түймесін басыңыз.
4. Ашылмалы тізімнен **Оқиғаларды файлға экспорттау** тармағын таңдаңыз.

Нәтижесінде, оқиғаларды экспорттау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Оқиғаларды таңдаудан жою

Оқиғаларды таңдаудан жою үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. Тінтуірді және **SHIFT** не **CTRL** пернелерін пайдалану арқылы жою қажет оқиғаларды таңдаңыз.
4. Таңдалған оқиғаларды келесі тәсілдердің бірімен жойыңыз:

   - Бөлектелген оқиғалардың кез келгенінің контекстік мәзірінен **Жою** тармағын таңдаңыз.

     Барлығын жою контекстік мәзір элементін таңдағанда, қайсысын жою үшін алдын ала таңдағаныңызға қарамастан, таңдаудан барлық көрсетілетін оқиғалар жойылады.

   - Егер бір оқиға таңдалса, **Оқиғаны жою** сілтемесі бойынша немесе таңдалған оқиғалармен жұмыс блогында бірнеше оқиға таңдалса, **Оқиғалар жойылуда** сілтемесі бойынша.

Нәтижесінде, таңдалған оқиғалар жойылады.

Бағдарламаларды пайдаланушылардың сұраулары бойынша ерекшеліктерге қосу

Егер сіз қате құлыпталған бағдарламалардың құлпын ашу үшін пайдаланушылардың сұрауларын алсаңыз, онда сіз осы бағдарламалар үшін Аномалияларды бейімделумен басқару ережелерінен ерекшелік жасай аласыз. Мұндай бағдарламалар енді пайдаланушылардың құрылғыларында құлыпталмайды. Басқару серверінің жұмыс аймағындағы **Мониторинг** қойыншасында пайдаланушылардың сұрауларының санын бақылауға болады.

Kaspersky Endpoint Security құлыптаған бағдарламаны пайдаланушылардың сұрауы бойынша ерекшеліктерге қосу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Оқиғалар** қойыншасын таңдаңыз.
3. **Оқиғаларды таңдау** ашылмалы тізімінен **Пайдаланушылардың сұраулары** тармағын таңдаңыз.
4. Ерекшеліктерге қосылатын бағдарламаларды қамтитын пайдаланушылардың сұрауының (немесе бірнеше пайдаланушылардың сұрауының) контекстік мәзірінен **Ерекшеліктерге қосу** тармағын таңдаңыз.

   Ерекшелікті қосу шебері қосылады. Шебердің қадамдарын орындаңыз.

Таңдалған қолданбалар клиент құрылғысын басқару серверімен келесі синхрондаудан кейін **"Смарт оқыту" күйіндегі ереже триггерлері** тізімінен (консоль тармағындағы **Қоймалар** бөлімінде) орындалады және тізімде енді көрсетілмейді.

Құрылғыны таңдаулары

Құрылғылардың күйі туралы ақпарат консоль ағашының **Құрылғы таңдаулары** қалтасында бар.

Құрылғы таңдаулары қалтасындағы ақпарат құрылғыларды таңдау тізімі түрінде ұсынылған. Әрбір таңдау белгілі бір шарттарға сәйкес келетін құрылғыларды қамтиды. Мысалы, **Критикалық күйі бар құрылғылар** таңдауы тек *Критикалық* күйі бар құрылғыларды ғана қамтиды. Бағдарлама орнатылғаннан кейін, **Құрылғы таңдаулары** қалтасы бірқатар стандартты таңдауларды қамтиды. Сіз құрылғылардың қосымша (пайдаланушы) таңдауларын жасай аласыз, таңдау параметрлерін файлға экспорттай аласыз, сондай-ақ файлдан импортталған параметрлермен таңдаулар жасай аласыз.

Құрылғы таңдауларын қарап шығу

Құрылғы таңдауларын көру үшін:

1. Консоль ағашында **Құрылғы таңдаулары** қалтасын таңдаңыз.
2. **Іріктемедегі құрылғылары** тізіміндегі қалтаның жұмыс аймағында өзіңізге қажетті құрылғы таңдауларын таңдаңыз.
3. **Таңдауды іске қосу** түймесін басыңыз.
4. **Таңдау нәтижелері** қойыншасын таңдаңыз.

Нәтижесінде, жұмыс аймағында таңдау параметрлеріне сәйкес келетін құрылғылардың тізімі көрсетіледі.

Құрылғылар тізіміндегі ақпаратты кез келген бағандағы деректердің өсуі немесе азаюы бойынша сұрыптауға болады.

Құрылғы таңдауларын конфигурациялау

Құрылғы таңдаулары параметрлерін конфигурациялау үшін:

1. Консоль ағашында **Құрылғы таңдаулары** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында **Таңдау** қойыншасына өтіп, реттелмелі құрылғы таңдаулары тізіміндегі өзіңізге қажетті құрылғы таңдауларын таңдаңыз.
3. **Таңдау сипаттары** түймесін басыңыз.
4. Ашылған сипаттар терезесінде келесі параметрлерді белгілеңіз:
   - Таңдаудың жалпы параметрлері.
   - Құрылғы осы таңдауға қосылуы үшін орындалуы керек шарттар. Шарттарды конфигурациялау үшін шарттардың атауын таңдап, **Сипаттар** түймесін басыңыз.
   - Қауіпсіздік параметрлері.
5. **OK** түймесін басыңыз.

   Параметрлер қолданылған және сақталған.

Төменде құрылғыларды таңдауға жатқызу шарттарының параметрлері сипатталған. Шарттар логикалық "немесе" бойынша біріктіріледі: ұсынылған шарттардың кем дегенде біреуін қанағаттандыратын құрылғылар таңдауға түседі.

Жалпы

Жалпы бөлімінде таңдау шартының атауын өзгертуге және осы шартты кері қайтару қажет пе екенін көрсетуге болады:

Таңдау шартын кері қайтару

Әдепкі бойынша, параметр өшірулі.

Бұл опцияны қоссаңыз, берілген таңдау шарты инверсияланады. Шартқа сәйкес келмейтін барлық құрылғылар таңдауға кіреді.

Келесі мысалда инверсия жұмысының логикасы көрсетілген:

- **Шарт**: құрылғыда Linux түріндегі операциялық жүйе және 00.0.000 құрастыру нөмірі бар.
- **Инверсияланған жағдай**: құрылғыда келесінің баламасы болатын NOT (Linux түрі және 00.0.000 құрастыру нөмірі) бар операциялық жүйе бар.

  NOT түріндегі Linux НЕМЕСЕ NOT 00.0.000 құрастыру нөмірі бар операциялық жүйе бар.

Осылайша таңдауға, мысалы, Windows түріндегі және 00.0.000 құрастыру нөмірі бар немесе Linux түріндегі және 00.0.000-ден басқа жинақ нөмірі бар құрылғылар кіреді.

Желі

Желі бөлімінде құрылғыларды олардың желілік деректері негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғының атауы немесе IP мекенжайы**

  Windows желісіндегі құрылғы атауы (NetBIOS атауы) немесе IPv4 мекенжайы не IPv6 мекенжайы.

- **Windows домені**

  Көрсетілген Windows доменіне кіретін барлық құрылғылар көрсетіледі.

- **Басқару тобы**

  Көрсетілген басқару тобына кіретін құрылғылар көрсетіледі.

- **Сипаттама**

  Құрылғы сипаттары терезесінде қамтылған мәтін: **Жалпы** бөлімінің **Сипаттама** өрісінде.

  Сипаттама мәтінінде келесі таңбаларды қолдануға болады:

  - Бір сөздің ішінде:

    - ***.** 0 немесе одан да көп таңбадан ұзын кез келген жолды алмастырады.

    Мысалы:

    Сервер, **Серверлік** сөздерін сипаттау үшін **Сервер*** жолын қолдануға болады.

    - **?.** Кез келген бір таңбаны ауыстырады.

    Мысалы:

    Құралдар немесе **Құралдан** сөздерін сипаттау үшін **Құралда?** жолын қолдануға болады.

Жұлдызша (*****) немесе сұрақ белгісі (**?**) мәтін сипаттамасында бірінші таңба ретінде қолданылуы мүмкін емес.

- Бірнеше сөздерді байланыстыру үшін:

  - Бос орын. Сипаттамаларында аталған сөздердің кез келгені бар барлық құрылғыларды көрсетеді.

  Мысалы:

  Қосалқы немесе **Виртуалдық** сөзін қамтитын сөйлемшені сипаттау үшін **Қосалқы Виртуалды** жолын қолдануға болады.

  - **+**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болуын білдіреді.

  Мысалы:

  Қосалқы сөзін де, **Виртуалды** сөзін де қамтитын сөйлемшені сипаттау үшін **+Қосалқы+Виртуалды** жолын қолдануға болады.

  - **-**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болмауын білдіреді.

  Мысалы:

  Қосалқы сөзі болуы, бірақ **Виртуалды** сөзі болмауы тиісті сөйлемшені сипаттау үшін **+Қосалқы-Виртуалды** жолын қолдануға болады.

  - **"<мәтін үзіндісі>"**. Тырнақшаға алынған мәтін үзіндісі мәтінде толығымен болуы керек.

  Мысалы:

  Қосалқы Сервер сөзтіркесін қамтитын сөйлемшені сипаттау үшін, **"Қосалқы Сервер"** жолын қолдануға болады.

- **IP ауқымы**

  Бұл параметр қосулы болса, енгізу өрістерінде сіз іздеген құрылғылар кіруі тиісті аралықтың бастапқы және соңғы IP мекенжайларын көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

Тегтер

Тегтер бөлімінде бұған дейін басқарылатын құрылғылардың сипаттамаларына қосылған кілт сөздер (тегтер) бойынша құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Кем дегенде бір көрсетілген тег сәйкес келген жағдайда қолдану**

  Егер бұл параметр қосулы болса, іздеу нәтижелерінде сипаттамасында таңдалған тегтердің кемінде біреуі бар құрылғылар көрсетіледі.

  Егер бұл параметр өшірулі болса, іздеу нәтижелерінде тек сипаттамаларында барлық таңдалған тегтері бар құрылғылар көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Тег болуы керек**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі бар құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Тег болмауы керек**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі жоқ құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

Active Directory

Active Directory бөлімінде құрылғыларды олардың Active Directory деректері негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғы Active Directory ұйымдық бөлімшесінде орналасқан**

  Бұл параметр қосулы болса, енгізу өрісінде көрсетілген Active Directory ұйым бірлігіндегі құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Еншілес ұйымдық бөлімшелерін қосу**

  Бұл параметр қосулы болса, доменнің көрсетілген ұйымдық бірлігінің еншілес бөлімшелеріне кіретін құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы Active Directory тобының мүшесі болып табылады**

  Егер бұл параметр қосулы болса, енгізу өрісінде көрсетілген Active Directory тобындағы құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

Желілік белсенділік

Желілік белсенділік бөлімінде құрылғыларды олардың желілік белсенділігі негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бұл құрылғы тарату нүктесі болып табылады**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға тарату нүктелері болып табылатын құрылғылар қосылады.
  - **Жоқ**. Тарату нүктелері ретінде әрекет ететін құрылғылар таңдауға кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверімен байланысты үзбеу**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Қосулы**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы қойылған құрылғыларды қамтиды.
  - **Өшірулі**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы алынған құрылғыларды қамтиды.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қосылым профилі ауыстырылды**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға қосылым профилін ауыстырып қосу нәтижесінде Басқару серверіне қосылған құрылғылар кіреді.
  - **Жоқ**. Таңдауға қосылым профилін ауыстыру нәтижесінде басқару серверіне қосылған құрылғылар кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверіне соңғы қосылу уақыты**

  Осы жалаушаны пайдаланып, Басқару серверіне соңғы қосылу уақыты бойынша құрылғыларды іздеу өлшемшартын белгілей аласыз.

  Егер жалауша қойылса, енгізу өрістерінде, клиент құрылғысында орнатылған Желілік агенттің Басқару серверіне соңғы қосылуы орындалған аралықтың мәндерін (күні мен уақыты) көрсетуге болады. Таңдауға белгіленген аралыққа сәйкес келетін құрылғылар қосылады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Жаңа құрылғылар желі сауалнамасымен анықталды**

  Соңғы бірнеше күнде желіде сауалнама өткізу кезінде табылған жаңа құрылғыларды іздеу.

  Егер бұл параметр қосулы болса, онда **Анықтау кезеңі (тәу)** өрісінде көрсетілген күндер санында құрылғыларды анықтау процесінде табылған жаңа құрылғылар ғана таңдауға қосылады.

  Егер бұл параметр өшірулі болса, онда құрылғыны анықтау процесінде табылған барлық құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы көрінеді**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Бағдарлама қазіргі уақытта желіде көрінетін құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қазіргі уақытта желіде көрінбейтін құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Бағдарлама

Бағдарлама бөлімінде құрылғыларды таңдалған басқарылатын қолданбаның негізінде таңдауға қосу шарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Ашылмалы тізімде, Kaspersky бағдарламасының атауы бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады.

  Тізімде, әкімшінің жұмыс станциясында басқару плагиндері орнатылған бағдарламалардың атаулары ғана берілген.

  Егер бағдарлама таңдалмаса, онда өлшемшарт қолданылмайды.

- **Бағдарламаның нұсқасы**

  Енгізу өрісінде Kaspersky бағдарламасы нұсқасының нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер нұсқа нөмірі көрсетілмесе, онда өлшемшарт қолданылмайды.

- **Критикалық жаңартудың атауы**

  Енгізу өрісінде бағдарлама үшін белгіленген жаңарту пакетінің атауы немесе нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер өріс толтырылмаса, онда өлшемшарт қолданылмайды.

- **Модульдердің соңғы рет жаңартылған уақыты**

  Бұл параметрдің көмегімен құрылғыларда орнатылған бағдарлама модульдерінің соңғы рет жаңартылған уақыты бойынша құрылғыларды іздеу өлшемшартын белгілеуге болады.

  Егер жалауша қойылса, енгізу өрістерінде құрылғыларда орнатылған бағдарлама модульдерінің соңғы жаңартылуы орындалған аралық мәндерін (күні мен уақыты) көрсетуге болады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Құрылғы Kaspersky Security Center арқылы басқарылады**

  Ашылмалы тізімде Kaspersky Security Center басқаратын құрылғыларды таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама Kaspersky Security Center басқаратын құрылғыларды таңдауды қамтиды.
  - **Жоқ**. Қолданба Kaspersky Security Center арқылы басқарылмайтын құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қауіпсіздік бағдарламасы орнатылған**

  Ашылмалы тізімде қауіпсіздік бағдарламасы орнатылған құрылғыны таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама, қауіпсіздік бағдарламасы орнатылған құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қауіпсіздік қолданбасы орнатылмаған барлық құрылғыны таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Операциялық жүйе

Операциялық жүйе бөлімінде, орнатылған операциялық жүйенің негізінде құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады.

- **Операциялық жүйенің нұсқасы**

  Егер жалауша қойылса, тізімнен операциялық жүйелерді таңдауға болады. Көрсетілген операциялық жүйелер орнатылған құрылғылар іздеу нәтижелеріне қосылады.

- **Операциялық жүйенің биттік өлшемі**

  Ашылмалы тізімде операциялық жүйенің биттік өлшемін таңдауға болады, оның болуы бойынша құрылғыға құрылғыны жылжыту ережесі қолданылады (**Белгісіз**, **x86**, **AMD64** немесе **IA64**). Әдепкі бойынша, тізімде бірде-бір нұсқа таңдалмаған, операциялық жүйенің биттік өлшемі белгіленбеген.

- **Операциялық жүйенің қызметтік бума нұсқасы**

  Бұл өрісте операциялық жүйенің пакет нұсқасын (*X.Y* форматында) көрсетуге болады, ол жылжыту ережесінің құрылғыға қалай қолданылатынын анықтайды. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **Операциялық жүйе құрастырылымы**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйенің құрастыру нөмірі. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық құрастыру нөмірлерін іздеуді конфигурациялауға болады.

- **Операциялық жүйе шығарылымының идентификаторы**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйе шығарылымының идентификаторы. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш шығарылым идентификаторы болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық шығарылым идентификаторы нөмірлерін іздеуді конфигурациялауға болады.

Құрылғының күйі

Құрылғының күйі бөлімінде басқарылатын қолданбадағы құрылғы күйінің сипаттамасына сәйкес құрылғыларды таңдауға қосу шарттарын конфигурациялауға болады:

- **Құрылғының күйі**

  Құрылғы күйлерінің бірін таңдауға болатын ашылмалы тізім: *OK*, *Критикалық* немесе *Ескерту*.

- **Құрылғы күйінің сипаттамасы**

  Бұл өрісте орындалса, құрылғыға келесі күйлердің бірін тағайындайтын шарттардың жанындағы құсбелгі ұяшықтарын таңдай аласыз: *OK, Критикалық* немесе *Ескерту*.

- **Бағдарлама анықтаған құрылғы күйі**

  Нақты уақыт режимінде қорғау тапсырмасы күйінің мәнін таңдауға болатын ашылмалы тізім. Нақты уақыт режимінде қорғау күйі көрсетілген құрылғылар таңдауға қосылады.

Қорғаныс компоненттері

Қорғаныс компоненттері бөлімінде құрылғыларды қорғаныс күйі бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Дерекқорлардың шығарылған күні**

  Осы параметр таңдалса, клиент құрылғыларын іздеу антивирустық дерекқордың шығарылу күні бойынша орындалады. Енгізу өрістерінде іздеу жүргізілетін уақыт аралығын белгілеуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Вирустарға соңғы рет тексеру уақыты**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу соңғы рет зиянды БҚ іздеу уақыты бойынша жүзеге асырылады. Енгізу өрістерінде зиянды БҚ іздеу соңғы рет жүргізілген аралықты көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Анықталған қауіптердің жалпы саны**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу табылған вирустар санына сәйкес жүзеге асырылады. Енгізу өрістерінде табылған вирустар санының төменгі және жоғарғы мәндерін орнатуға болады.

  Әдепкі бойынша, параметр өшірулі.

Бағдарламалар тізімдемесі

Бағдарламалар тізімдемесі бөлімінде қандай қолданбалар орнатылғанына байланысты құрылғыларды іздеу шарттарын реттеуге болады:

- **Бағдарлама атауы**

  Бағдарламаны таңдауға болатын ашылмалы тізім. Көрсетілген бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарламаның нұсқасы**

  Таңдалған бағдарламаның нұсқасын көрсететін енгізу өрісі.

- **Өндіруші**

  Құрылғыда орнатылған бағдарламаның өндірушісін таңдауға болатын ашылмалы тізім.

- **Бағдарлама күйі**

  Бағдарлама күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған бағдарлама орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Жаңарту бойынша іздеу**

  Егер бұл параметр қосулы болса, іздеу сіз іздеген құрылғыларда орнатылған бағдарламаларды жаңарту деректері бойынша орындалады. Жалауша қойылғаннан кейін, **Бағдарлама атауы**, **Бағдарламаның нұсқасы** және **Бағдарлама күйі** өрістерінің орнына сәйкесінше **Жаңартудың атауы**, **Жаңартудың нұсқасы** және **Күйі** өрістері көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Үйлесімді емес қауіпсіздік бағдарламасының атауы**

  Үшінші тарап қауіпсіздік бағдарламаларын таңдауға болатын ашылмалы тізім. Іздеу кезінде, таңдалған бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарлама тегі**

  Ашылмалы тізімнен бағдарлама тегін таңдауға болады. Сипаттамада таңдалған тегі бар бағдарламалар орнатылған барлық құрылғылар құрылғылар таңдауына қосылады.

- **Көрсетілген тегтерсіз құрылғыларға қолдану**

  Параметр қосулы болса, онда таңдауға, сипаттамасында таңдалған тегтері жоқ құрылғылар қосылады.

Бұл параметр өшірулі болса, өлшемшарт қолданылмайды.

Әдепкі бойынша, параметр өшірулі.

Жабдық тізімдемесі

Жабдық тізімдемесі бөлімінде құрылғыларды оларға орнатылған жабдық бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғы**

  Ашылмалы тізімнен жабдық түрін таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Өндіруші**

  Ашылмалы тізімнен жабдық өндірушісінің атауын таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Құрылғы атауы**

  Windows желісіндегі құрылғының атауы. Көрсетілген атауы бар құрылғы таңдауға қосылады.

- **Сипаттама**

  Құрылғының немесе жабдықтың сипаттамасы. Өрісте көрсетілген сипаттамасы бар құрылғылар таңдау құрамына енгізіледі.

  Құрылғының сипаттамасын құрылғының сипаттары терезесінде еркін түрде енгізуге болады. Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Құрылғы өндірушісі**

  Құрылғы өндірушісінің атауы. Өрісте көрсетілген өндіруші жасаған құрылғылар таңдау құрамына енгізіледі.

  Өндірушінің атауын құрылғының сипаттары терезесінде енгізуге болады.

- **Сериялық нөмір**

  Өрісте көрсетілген сериялық нөмірі бар жабдық таңдауға қосылады.

- **Қойма нөмірі**

  Өрісте көрсетілген қойма нөмірі бар жабдық таңдауға қосылады.

- **Пайдаланушы**

  Өрісте көрсетілген пайдаланушының аппараттық жасақтамасы таңдауға қосылады.

- **Орналасуы**

  Құрылғының немесе жабдықтың орналасқан жері (мысалы, кеңседе немесе филиалда). Өрісте көрсетілген жерде орналасқан компьютерлер немесе басқа құрылғылар таңдау құрамына кіреді.

  Жабдықтың орналасуын жабдықтың сипаттары терезесінде еркін түрде енгізуге болады.

- **Орталық процессор жиілігі, МГц түрінде**

  Орталық процессор жиіліктері ауқымы. Енгізу өрістеріндегі (қоса алғанда) жиіліктер ауқымына сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Орталық процессордың виртуалды ядролар саны**

  Орталық процессордың виртуалды ядролар саны ауқымы. Енгізу өрістеріндегі (қоса алғанда) ауқымға сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Қатты дискінің көлемі, ГБ түрінде**

  Құрылғының қатты дискісі көлемі мәндерінің ауқымы. Енгізу өрістеріндегі (қоса алғанда) ауқымға сәйкес келетін қатты дискілері бар құрылғылар таңдау құрамына енгізіледі.

- **Жедел жадтың көлемі, МБ түрінде**

  Құрылғының ЖЖҚ өлшеміне арналған мәндер ауқымы. Осы енгізу өрістеріндегі (инклюзивті) ауқымға сәйкес келетін ЖЖҚ-сы бар құрылғылар таңдауға қосылады.

Виртуалды машиналар

Виртуалды машиналар бөлімінде, бұл құрылғылардың виртуалды машиналар немесе Virtual Desktop Infrastructure бөлігі екендігіне байланысты құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Виртуалды машина болып табылады**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Маңызды емес**.
  - **Жоқ**. Виртуалды машиналар емес құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

  Ашылмалы тізімнен виртуалды машина өндірушісін таңдауға болады.

  Бұл ашылмалы тізім **Виртуалды машина болып табылады** ашылмалы тізімінде **Иә** немесе **Маңызды емес** мәні таңдалған болса қолжетімді.

- **Virtual Desktop Infrastructure бөлігі**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Маңызды емес**.
  - **Жоқ**. Virtual Desktop Infrastructure-дың бөлігі болып табылмайтын құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар Virtual Desktop Infrastructure (VDI) бөлігі болуы тиіс.

Осалдықтар мен жаңартулар

Осалдықтар мен жаңартулар бөлімінде, құрылғыларды Windows Update жаңарту көздері бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

WUA Басқару серверіне ауысты

Ашылмалы тізімнен келесі іздеу нұсқаларының бірін таңдауға болады:

- **Иә**. Егер бұл нұсқа таңдалса, іздеу нәтижелеріне Windows Update жаңартуларын Басқару серверінен алатын құрылғылар кіреді.
- **Жоқ**. Бұл нұсқа таңдалса, нәтижелер жаңартуларды Windows Update арқылы басқа дереккөздерден алатын құрылғыларды қамтиды.

Пайдаланушылар

Пайдаланушылар бөлімінде құрылғыларды операциялық жүйеге кірген пайдаланушылардың есептік жазбалары бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады.

- **Жүйеге соңғы кірген пайдаланушы**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде пайдаланушы есептік жазбасын көрсетуге болады. Іздеу нәтижелеріне, жүйеге соңғы рет кіруді көрсетілген пайдаланушы орындаған құрылғылар кіреді.

- **Жүйеге кемінде бір рет кірген пайдаланушы**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде пайдаланушы есептік жазбасын көрсетуге болады. Іздеу нәтижелеріне, аталған пайдаланушы жүйеге кемінде бір рет кірген құрылғылар кіреді.

Басқарылатын бағдарламалардағы күйге әсер ететін мәселелер

Басқарылатын бағдарламалардағы күйге әсер ететін мәселелер бөлімінде басқарылатын қолданба анықтаған ықтимал мәселелер тізіміне сәйкес құрылғыларды таңдауға қосу шарттарын көрсетуге болады. Егер сіз таңдаған құрылғыда кем дегенде бір мәселе болса, құрылғы таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген мәселені таңдағанда, сізде барлық тізімдерде осы мәселені автоматты түрде таңдау мүмкіндігі болады.

Құрылғы күйінің сипаттамасы

Сіз басқарылатын бағдарламалар күйлерінің сипаттамасы үшін жалаушаларды қоя аласыз, оларды алған кезде құрылғылар таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген күйді таңдағанда, сізде барлық тізімдерде осы күйді автоматты түрде таңдау мүмкіндігі болады.

Басқарылатын бағдарламалардың құрамдастарының күйлері

Басқарылатын бағдарламалардың құрамдастарының күйлері бөлімінде басқарылатын қолданбалар құрамдастарының күйлеріне сәйкес құрылғыларды таңдауға қосу шарттарын конфигурациялауға болады:

- **Деректердің жайылып кетуіне жол бермеу күйі**

  Деректердің жайылып кетуінен қорғау құрамдасының күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Бірлескен жұмыс серверлерінің қорғаныс күйі**

  Бірлескен жұмыс серверлері үшін қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз*, *Тоқтатылды*, *Іске қосылды, Кідіртілді*, *Орындалуда*, *Сәтсіз аяқталды*).

- **Пошталық серверлердің антивирустық қорғаныс күйі**

  Пошта серверінің қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Endpoint Sensor күйі**

  Құрылғыларды Endpoint Sensor құрамдасының күйі бойынша іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

Шифрлау

Шифрлау алгоритмі

Advanced Encryption Standard (AES) симметриялық блоктық шифрлау алгоритмі стандарты. Ашылмалы тізімнен шифрлау кілтінің өлшемін таңдай аласыз (56 Бит, 128 Бит, 192 Бит немесе 256 Бит).

Қолжетімді мәндер: *AES56*, *AES128*, *AES192*, және *AES256*.

Бұлттық сегменттер

Бұлттық сегменттер бөлімінде, бұлттық сегменттерге сәйкес құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғы бұлттық сегментте орналасқан**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде іздеу сегментін көрсетуге болады.

  Қосалқы нысандарды қосу параметрі де қосулы болса, іздеу көрсетілген сегменттің барлық салынған нысандары бойынша жүргізіледі.

  Іздеу нәтижелеріне тек таңдалған сегменттегі құрылғылар кіреді.

- **Құрылғы API арқылы табылды**

  Ашылмалы тізімнен, құрылғының API құралдарымен анықталады ма екенін таңдауға болады:

  - **AWS**. Құрылғы AWS API арқылы табылды, яғни құрылғы AWS бұлтты ортасында орналасқан.
  - **Azure**. Құрылғы Azure API арқылы табылды, яғни құрылғы Azure бұлтты ортасында орналасқан.
  - **Google Cloud.** Құрылғы Google API арқылы табылды, яғни құрылғының Google Cloud ортасында орналасқаны анық.
  - **Жоқ**. Құрылғыны AWS, Azure немесе Google API пайдалану арқылы анықтау мүмкін емес, яғни ол бұлттық ортадан тыс немесе бұлттық ортада, бірақ оны API арқылы анықтау мүмкін емес.
  - **Көрсетілмеген**. Бұл шарт қолданылмайды.

Бағдарлама құрамдастары

Бұл бөлімде Басқару консолінде орнатылған тиісті басқару плагиндері бар бағдарламалар құрамдастарының тізімі келтірілген.

Бағдарлама құрамдастары қойындысында таңдалған қолданбаға қатысты құрамдастар күйлері мен нұсқа нөмірлеріне сәйкес құрылғыларды таңдауға қосу шарттарын көрсетуге болады.

- **Күйі**

  Басқарылатын бағдарлама Басқару серверіне жіберген құрамдастың күйіне сәйкес құрылғыларды іздеу. Сіз келесі күйлердің бірін таңдай аласыз: *Құрылғыдан деректер жоқ*, *Тоқтатылды*, *Іске қосылды*, *Кідіртілді*, *Орындалуда*, *Сәтсіз аяқталды* немесе *Орнатылмаған*. Егер басқарылатын құрылғыда орнатылған бағдарламаның таңдалған құрамдасы көрсетілген күйге ие болса, құрылғы құрылғыны таңдауға кіреді.

  Бағдарламалар жіберген күйлер:

  - *Іске қосылды* – құрамдас қазіргі уақытта инициализация процесінде.
  - *Орындалуда* – құрамдас қосулы және дұрыс жұмыс істейді.
  - *Кідіртілді* – құрамдас, мысалы, пайдаланушы басқарылатын бағдарламада қорғанысты кідірткеннен кейін кідіртіледі.
  - *Сәтсіз аяқталды* – құрамдастың операциясын орындау кезінде қате пайда болды.
  - *Тоқтатылды* – құрамдас өшірілген және қазіргі уақытта жұмыс істемейді.
  - *Орнатылмаған* – пайдаланушы бағдарламаны іріктеп орнату кезінде орнату құрамдасын таңдамады.

  Басқа күйлерден айырмашылығы: *Құрылғыдан келген деректер жоқ* күйін қолданбалар жібермейді. Бұл параметр, бағдарламаларда таңдалған құрамдас күйі туралы ақпарат жоқ екенін көрсетеді. Мысалы, бұл жағдай, таңдалған құрамдас құрылғыда орнатылған бағдарламалардың ешқайсысына тиесілі болмаса немесе құрылғы өшірулі болса, орын алуы мүмкін.

- **Нұсқа**

  Тізімде таңдалған құрамдас нұсқасының нөміріне сәйкес құрылғыларды іздеу. Сіз `3.4.1.0` сияқты нұсқа нөмірін енгізе аласыз, содан кейін таңдалған құрамдастың тең, анағұрлым ерте немесе анағұрлым кейінгі нұсқасы болуы керек пе екенін көрсете аласыз. Сондай-ақ, іздеуді көрсетілген нұсқадан басқа құрамдастың барлық нұсқалары бойынша конфигурациялауға болады.

Құрылғы таңдаулары параметрлерін файлға экспорттау

Құрылғы таңдаулары параметрлерін мәтіндік файлға экспорттау үшін:

1. Консоль ағашында **Құрылғы таңдаулары** қалтасын таңдаңыз.
2. **Таңдау** қойыншасындағы қалтаның жұмыс аймағында реттелмелі құрылғы таңдаулары тізіміндегі өзіңізге қажетті құрылғы таңдауларын таңдаңыз.

   Параметрлерді тек пайдаланушы жасаған құрылғы таңдауларынан экспорттауға болады.

3. **Таңдауды іске қосу** түймесін басыңыз.

4. **Таңдау нәтижелері** қойыншасында **Параметрлерді экспорттау** түймесін басыңыз.

5. Ашылған **Басқаша сақтау** терезесінде таңдау параметрлерін экспорттау үшін файл атауын белгілеңіз, файл сақталатын қалтаны көрсетіңіз және **Сақтау** түймесін басыңыз.

Құрылғыны таңдау параметрлері көрсетілген файлға сақталады.

Құрылғы таңдауларын жасау

Құрылғы таңдауларын жасау үшін:

1. Консоль ағашында **Құрылғы таңдаулары** қалтасын таңдаңыз.

2. Қалтаның жұмыс аймағында **Кеңейтілген** түймесін басып, ашылмалы тізімнен **Таңдау жасау** тармағын таңдаңыз.

3. Ашылған **Жаңа құрылғыны таңдау** терезесінде жасалып жатқан таңдаудың атауын көрсетіп, **OK** түймесін басыңыз.

Нәтижесінде, консоль ағашында **Құрылғы таңдаулары** қалтасында сіз көрсеткен атпен жаңа қалта жасалады. Әдепкі бойынша, жасалған құрылғы таңдауы, осы таңдаудың жасалуына себеп болған Сервердің басқару топтарына кіретін барлық құрылғыларды қамтиды. Таңдауда тек сізді қызықтыратын құрылғылар көрсетілуі үшін таңдау параметрлерін **Таңдау сипаттары** түймесі бойынша конфигурациялау керек.

Импортталған параметрлер бойынша құрылғылар таңдауын жасау

Импортталған параметрлер бойынша құрылғылар таңдауын жасау үшін:

1. Консоль ағашында **Құрылғы таңдаулары** қалтасын таңдаңыз.

2. Қалтаның жұмыс аймағында **Кеңейтілген** түймесін басып, ашылмалы тізімнен **Файлдан таңдауды импорттау** тармағын таңдаңыз.

3. Ашылған терезеде таңдау параметрлерін импорттағыңыз келетін файлдың жолын көрсетіңіз. **Ашу** түймесін басыңыз.

Құрылғы таңдаулары қалтасында **Жаңа таңдау** енгізілімі жасалады. Жаңа таңдау параметрлері көрсетілген файлдан импортталған.

Жаңа таңдау қалтасында **Құрылғы таңдаулары** атты таңдау бұрыннан бар болса, жасалған таңдаудың атына түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы қосылады.

Таңдаудағы басқару топтарынан құрылғыларды жою

Құрылғы үлгісімен жұмыс істегенде, құрылғыларды жою қажет басқару топтарымен жұмыс істеуге өтпей-ақ, құрылғыларды басқару топтарынан тікелей таңдаудың өзінде жоюға болады.

Басқару топтарынан құрылғыларды жою үшін:

1. Консоль ағашында **Құрылғы таңдаулары** қалтасын таңдаңыз.
2. Жойылуы қажет құрылғыларды **Shift** немесе **Ctrl** пернелерінің көмегімен таңдаңыз.
3. Таңдалған құрылғыларды басқару топтарынан келесі тәсілдердің бірімен жойыңыз:
   - Бөлектелген құрылғылардың кез келгенінің контекстік мәзірінен **Жою** тармағын таңдаңыз.
   - **Әрекетті орындау** түймесін басыңыз да, ашылатын тізімнен **Топтан жою** мәнін таңдаңыз.

Нәтижесінде, таңдалған құрылғылар өздері кіретін басқару топтарынан жойылады.

Бағдарламаларды орнату және жою мониторингі

Сіз басқарылатын құрылғыларда белгілі бір бағдарламаларды, мысалы, белгілі бір браузерді орнатуды және жоюды басқара аласыз. Осы функцияны қолдану үшін, сіз бағдарламалар тізімдемесіндегі бағдарламаларды бақыланатын бағдарламалар тізіміне қоса аласыз. Бақыланатын бағдарламаны орнату немесе жою кезінде, Желілік агент тиісті оқиғаларды жариялайды: **Бақыланатын бағдарлама орнатылды** или **Бақыланатын бағдарлама жойылды**. Сіз, мысалы, оқиғалар таңдауын немесе есептерді қолдана отырып, осы оқиғаларды бақылай аласыз.

Осы оқиғалар Басқару серверінің дерекқорында сақталса ғана, оларды бақылай аласыз.

Бағдарламаны бақыланатын бағдарламалар тізіміне қосу үшін:

1. Консоль ағашында, **Кеңейтілген** → **Бағдарламаларды басқару** қалтасында **Бағдарламалар тізімдемесі** салынған қалтасын таңдаңыз.
2. Көрсетілген бағдарламалар тізімінің үстінен **Бағдарламалар тізімдемесінің сипаттар терезесін көрсету** түймесін басыңыз.
3. Ашылған **Бақыланатын бағдарламалар** терезесінде **Қосу** түймесін басыңыз.
4. Ашылған **Бағдарлама атауын таңдаңыз** терезесінде, бағдарламалар тізімдемесінде қандай бағдарламалар үшін орнату мен жоюды бақылағыңыз келетінін таңдаңыз.
5. **Бағдарлама атауын таңдаңыз** терезесінде **OK** түймесін басыңыз.

Бағдарламалар тізімін конфигурациялағаннан кейін және бақыланатын бағдарлама сіздің ұйымыңыздағы құрылғыларға орнатылғаннан немесе олардан жойылғаннан кейін, сіз тиісті оқиғаларды, мысалы, Соңғы оқиғалар оқиғалар таңдауының көмегімен бақылай аласыз.

Kaspersky Security Center құрамдастарының оқиғалары

Kaspersky Security Center әрбір құрамдасының өзіндік оқиғалар түрлерінің жиынтығы бар. Бұл бөлімде Kaspersky Security Center басқару серверінде, желілік агентте және iOS MDM серверінде орын алатын оқиғалардың түрлері берілген. Kaspersky бағдарламаларында орын алатын оқиғалар түрлері бұл бөлімде атап көрсетілмеген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрі сипаттамасы деректерінің құрылымы

Оқиғалардың әр түрі үшін оның аты, идентификаторы, әріптік коды, сипаттамасы және әдепкі бойынша сақтау уақыты көрсетіледі.

- **Оқиға түрінің көрсетілетін атауы**. Бұл мәтін Kaspersky Security Center бағдарламасында оқиғаларды орнатқан кезде және олар пайда болған кезде көрсетіледі.
- **Оқиға түрі идентификаторы**. Бұл сандық код үшінші тарап оқиғаларын талдау құралдарын қолдана отырып, оқиғаларды өңдеуде қолданылады.
- **Оқиға түрі** (әріптік код). Бұл код Kaspersky Security Center дерекқорының жария көріністерін пайдалана отырып, оқиғаларды қарау және өңдеу кезінде және оқиғаларды SIEM жүйелеріне экспорттау кезінде пайдаланылады.
- **Сипаттамасы**. Бұл мәтінде оқиға болған кездегі жағдайдың сипаттамасы және бұл жағдайда не істеуге болатыны туралы сипаттама келтірілген.
- **Әдепкі бойынша сақтау мерзімі**. Бұл, оқиға Басқару серверінің дерекқорында сақталатын және Басқару сервері оқиғаларының тізімінде көрсетілетін күндер саны. Осы кезең аяқталғаннан кейін, оқиға жойылады. Егер оқиғаны сақтау уақытының мәні 0 болып көрсетілсе, мұндай оқиғалар тіркеледі, бірақ Басқару сервері оқиғалары тізімінде көрсетілмейді. Егер сіз осындай оқиғаларды операциялық жүйенің оқиғалар журналында сақтауды конфигурациялаған болсаңыз, оларды сол жерден таба аласыз.

  Оқиғаларды сақтау уақытын өзгертуге болады:

  - Басқару консолі: Оқиғаны сақтау мерзімін конфигурациялау.
  - Kaspersky Security Center Web Console: Оқиғаны сақтау мерзімін конфигурациялау.

Басқа деректер келесі өрістерді қамтуы мүмкін:

- **event_id**: дерекқордағы оқиғаның автоматты түрде жасалған және тағайындалған бірегей нөмірі; **Оқиға түрінің идентификаторымен** шатастырмау керек.
- **task_id**: орындау нәтижесінде оқиға туындаған тапсырма идентификаторы (ондай бар болса).
- **severity**: келесі маңыздылық деңгейлерінің бірі (маңыздылықтың өсуі ретімен):

  0) Жол бергісіз маңыздылық деңгейі.

  1) Ақпараттық.

  2) Ескерту.

  3) Қате.

  4) Критикалық.

Басқару сервері оқиғалары

Бұл бөлімде Басқару сервері оқиғалары туралы ақпарат бар.

Басқару серверінің критикалық оқиғалары

Төмендегі кестеде **Критикалық** маңыздылық деңгейі бар Kaspersky Security Center Басқару сервері оқиғаларының түрлері келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару консолиндегі басқару серверінің сипаттары терезесінде портты көрсетсеңіз, **Kaspersky Security Center қызметі** Promtheus (бақылау және ескерту жүйесі) қабылдайтын оның көрсеткіштері мен критикалық оқиғаларын жариялайды. Prometheus көрсеткіштерді және критикалық оқиғаларды алады, содан кейін әрбір оқиға үшін ескертулер жасайды.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензиялық шектеу асырылды	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Күніне бір рет Kaspersky Security Center бағдарламасы лицензиялық шектеудің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын лицензиялық бірліктердің жалпы санының 110%-нан асса туындайды. Осы оқиға туындаса да, клиент құрылғылары қорғалған. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	180 күн
Вирустық шабуыл	26 (Файл қауіптерінен қорғаныс құрамдасы үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	180 күн
Вирустық шабуыл	27 (Пошта қауіптерінен қорғаныс құрамдасы үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Вирустық шабуыл	28 (желілік экран үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	180 күн
Құрылғы басқарылмайтын күйге айналды	4111	KLSRV_HOST_OUT_CONTROL	Осы түрдегі оқиғалар, басқарылатын құрылғы желіде көрініп тұрса да, Басқару сервері белгіленген кезең ішінде қосылмаған жағдайда туындайды. Құрылғыда Желілік агенттің дұрыс жұмыс істеуіне не кедергі келтіретінін анықтаңыз. Ықтимал себептеріне желі ақаулары және құрылғыдан Желілік агентті жою кіруі мүмкін.	180 күн
Құрылғының күйі: "Критикалық"	4113	KLSRV_HOST_STATUS_CRITICAL	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Критикалық* күйі тағайындалса туындайды. Сіз шарттарды конфигурациялай аласыз, оларды орындау кезінде құрылғының күйі *Критикалық* болып өзгереді.	180 күн
Кілт файлы қара тізімге қосылды	4124	KLSRV_LICENSE_BLACKLISTED	Осы түрдегі оқиғалар, Kaspersky бағдарламасы сіз қолданып жатқан белсендіру кодын немесе лицензиялық кілтті тыйым салынғандар тізіміне қосқан болса туындайды. Толығырақ ақпарат алу үшін Техникалық қолдау қызметіне жүгініңіз.	180 күн
Шектелген функционалдылық режимі	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Осы түрдегі оқиғалар, Kaspersky Security Center бағдарламасы Ұялы құрылғыларды басқару және Осалдықтар мен патчтарды басқару мүмкіндігінің қолдауынсыз, базалық функционалдылық режимінде жұмыс істей бастаса туындайды. Төменде себептер және оқиғаға берілген тиісті жауаптар келтірілген: • Лицензия мерзімі өтті. Kaspersky Security Center толық функционалдылығына лицензия беріңіз (Басқару серверіне белсендіру кодын немесе кілт файлын қосыңыз). • Басқару сервері ұсынылған лицензия бойынша қолданылуы мүмкін саннан көп құрылғылар санын басқарады. Құрылғыларды бір Сервердің басқару топтарының құрамынан басқа Сервердің басқа топтарына жылжытыңыз (басқа Сервердің лицензиялық шектеуі асып кетпесе).	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензияның қолданылу мерзімі жақында аяқталады	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Осы түрдегі оқиғалар, коммерциялық лицензияның жарамдылық мерзімінің аяқталу күні жақындаса туындайды. Күніне бір рет Kaspersky Security Center бағдарламасы лицензияның лицензия мерзімінің өтпегенін тексеріп тұрады. Осы түрдегі оқиғалар 30 күн, 15 күн, 5 күн және 1 күн бұрын, лицензия мерзімі аяқталғанға дейін жарияланады. Сіз күндер санын өзгерте алмайсыз. Басқару сервері лицензияның жарамдылық мерзімінің аяқталу күніне дейін көрсетілген күні өшірілсе, оқиға келесі күнге дейін жарияланбайды. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, Kaspersky Security Center бағдарламасы Базалық функционалдылық режимінде жұмыс істейді. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Резервттегі лицензиялық кілт Басқару серверіне қосылғанына көз жеткізіңіз. • Жазылымды қолдансаңыз, оның мерзімін ұзартыңыз. Провайдерге алғы төлем уақтылы төленген болса, шектелмеген жазылым автоматты түрде ұзартылады.	180 күн
Сертификаттың жарамдылық мерзімі бітті	4132	KLSRV_CERTIFICATE_EXPIRED	Бұл түрдегі оқиғалар мобильдік құрылғылардағы клиент сертификатының мерзімі аяқталғанда орын алады.	180 күн
Басқару сервері сертификатының мерзімі аяқталды.	6129	ServerCertificateExpired	Осы түрдегі оқиғалар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару сервері сертификаттарының жарамдылық мерзімі аяқталғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	180 күн
Kaspersky қолданбасының модульдеріне арналған жаңартулар қайтарылды	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Kaspersky техникалық қолдау қызметінің мамандары үзіліссіз жаңартуларды қайтарып алса (бұл жаңартулар үшін *Қайтарылған* күйі көрсетіледі); мысалы, оларды жаңа нұсқаға жаңарту қажет болса, осы түрдегі оқиғалар пайда болады. Оқиға Kaspersky Security Center патчтарына қатысты емес және Kaspersky басқарылатын бағдарлама модульдеріне жатпайды. Оқиға жаңартулардың орнатылмауы себебін қамтиды.	180 күн
Аудит: SIEM серверіне экспорттау сәтсіз аяқталды	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Осы түрдегі оқиғалар, SIEM жүйесіне оқиғаларды экспорттау SIEM жүйесіне қосылу қатесіне байланысты сәтсіз аяқталғанда орын алады.	180 күн

Басқару серверінің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center Басқару сервері оқиғаларының түрлері келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару серверінің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Орындау уақытының қатесі	4125	KLSRV_RUNTIME_ERROR	Осы түрдегі оқиғалар белгісіз мәселелерден туындайды. Көбінесе бұл ДҚБЖ мәселелері, желімен байланысты мәселелер, сондай-ақ бағдарламалық және аппараттық жасақтамамен байланысты басқа да мәселелер. Оқиға туралы толық ақпаратты оның сипаттамасынан табуға болады.	180 күн
Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі асырылды	4126	KLSRV_INVLICPROD_EXCEDED	Басқару сервері осындай түрдегі оқиғаларды мерзімді түрде (сағат сайын) жасайды. Kaspersky Security Center бағдарламасында үшінші тарап бағдарламаларының лицензиялық кілттерін басқарсаңыз және орнату саны үшінші тарап бағдарламасының лицензиялық кілтінде белгіленген шектен асып кетсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Үшінші тарап бағдарламасын, ол қолданылмайтын құрылғылардан жойыңыз. • Үшінші тарап лицензиясын көптеген құрылғыларға қолданыңыз. Лицензиялы бағдарламалар тобының функционалдылығын қолдана отырып, лицензиялы бағдарламалардың лицензиялық кілттерін басқара аласыз. Лицензиялы бағдарламалар тобына, сіз белгілеген өлшемшарттарға сай келетін үшінші тарап бағдарламалары кіреді.	180 күн
Бұлттық сегментте сауалнаманы орындау мүмкін болмады	4143	KLSRV_KLCLOUD_SCAN_ERROR	Осы түрдегі оқиғалар, Басқару сервері бұлтты ортадағы желі сегментінде сауалнама өткізе алмаған жағдайда туындайды. Оқиғаның сипаттамасындағы ақпаратты оқып, оларға тиісінше ден қойыңыз.	Сақталмайды

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Белгіленген қалтаға жаңартуларды көшіру мүмкін болмады	4123	KLSRV_UPD_REPL_FAIL	Бағдарламалық жасақтама жаңартулары ортақ қатынасы бар қалтаға (немесе қалталарға) көшірілсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Қалтаға (немесе қалталарға) қатынасу үшін пайдаланылатын пайдаланушы есептік жазбасының жазу құқығы бар-жоғын тексеріңіз. • Қалта(лар)ға арналған пайдаланушы аты және/немесе құпиясөз өзгергенін тексеріңіз. • Интернет қосылымын тексеріңіз, себебі бұл оқиғаның себебі болуы мүмкін. Дерекқорлар мен бағдарламалық модульдерді жаңарту жөніндегі нұсқауларды орындаңыз.	180 күн
Дискіде бос орын жоқ	4107	KLSRV_DISK_FULL	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғының қатты дискісінде диск кеңістігі таусылып бара жатқан жағдайда туындайды. Құрылғыдағы диск кеңістігін босатыңыз.	180 күн
Ортақ қалта қолжетімсіз	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Осы түрдегі оқиғалар, Басқару серверінің ортақ қатынасы бар қалтасы қолжетімді болмағанда туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің (ортақ қатынасы бар қалта орналасқан) қосулы және қолжетімді екеніне көз жеткізіңіз. • Қалтаға арналған пайдаланушы аты және/немесе құпиясөз өзгертілгенін тексеріңіз. • Желі қосылымын тексеріңіз.	180 күн
Басқару серверінің дерекқоры қолжетімсіз	4109	KLSRV_DATABASE_UNAVAILABLE	Осы түрдегі оқиғалар Басқару сервері дерекқоры қолжетімсіз болған жағдайда пайда болады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • SQL сервері орнатылған қашықтағы сервердің қолжетімді ме екенін тексеріңіз. • ДҚБЖ оқиғалар журналдарын қарап шығыңыз және Басқару сервері дерекқорының қолжетімсіздігінің себебін табыңыз. Мысалы, алдын алу жұмыстарына байланысты, SQL Server сервері орнатылған қашықтағы сервер қолжетімді болмауы мүмкін.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Басқару серверінің дерекқорында бос орын жоқ	4110	KLSRV_DATABASE_FULL	Бұл түрдегі оқиғалар Басқару сервері дерекқорында бос орын болмаса пайда болады. Басқару серверінің дерекқоры толып кетсе және дерекқорға одан әрі жазу мүмкін болмаса, Басқару сервері жұмыс істемейді. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиғаға ден қоюдың тиісті тәсілдері келтірілген: • Сіз SQL Server Express Edition қолданасыз: SQL Server Express құжаттамасында, қолданылатын нұсқа үшін дерекқор өлшеміне қойылған шектеуді тексеріңіз. Басқару серверіңіздің дерекқоры дерекқор өлшемінің шегінен асып кеткен болса керек. Басқару серверінің дерекқорында сақталатын оқиғалар санын шектеңіз. Басқару сервері дерекқорында бағдарламаларды басқару құрамдасы жіберген оқиғалар өте көп. Басқару серверінің дерекқорында Бағдарламаларды басқару құрамдасының оқиғаларын сақтауға қатысты Kaspersky Endpoint Security for Windows саясатының параметрлерін өзгертуге болады. • SQL Server Express Edition жүйесінен ерекшеленетін ДҚБЖ қолданасаңыз: Басқару серверінің дерекқорында сақталатын оқиғалар санын шектемеңіз. Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	180 күн

Басқару серверінің ескерту оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Жиі болатын оқиға анықталды		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Басқару сервері басқарылатын құрылғыда жиі болатын оқиғаларды тіркейтін болса, осы түрдегі оқиғалар орын алады. Қосымша ақпаратты келесі бөлімдерден қараңыз: Жиі оқиғаларды бұғаттау.	90 күн
Лицензиялық шектеу асырылды	4098	KLSRV_EV_LICENSE_CHECK_100_110	Күніне бір рет Kaspersky Security Center бағдарламасы лицензиялық шектеудің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын бірліктердің жалпы саны 100%-дан 110%-ға дейін құраса туындайды. Осы оқиға туындаса да, клиент құрылғылары қорғалған. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	90 күн
Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Осы түрдегі оқиғалар, басқарылатын құрылғы бірнеше уақыт бойы белсенді емес болған кезде туындайды. Көбінесе, басқарылатын құрылғы істен шыққан жағдайда туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Құрылғыны басқарылатын құрылғылар тізімінен қолмен жойыңыз. • Басқару консолі көмегімен немесе Kaspersky Security Center Web Console көмегімен **Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды** оқиғасы жасалатын уақыт аралығын көрсетіңіз. • Құрылғы Басқару консолінің немесе Kaspersky Security Center Web Console веб-консолінің көмегімен автоматты түрде жойылатын уақыт аралығын көрсетіңіз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Құрылғылар атауларының қайшылығы	4102	KLSRV_EVENT_HOSTS_CONFLICT	Осы түрдегі оқиғалар, егер Басқару сервері екі немесе одан да көп басқарылатын құрылғыны бір құрылғы ретінде қарастырған кезде туындайды. Көбінесе, клондалған қатты диск бағдарламаларды басқарылатын құрылғыларда орналастыру үшін және Желілік агентті эталонды құрылғыда бөлектелген дискіні клондау режиміне ауыстырып қоспай қолданылған кезде туындайды. Бұл мәселені болдырмау үшін, осы құрылғының қатты дискісін клондаудың алдында Желілік агентті эталонды құрылғыда дискіні клондау режиміне ауыстырып қосыңыз.	90 күн
Құрылғының күйі: "Ескерту"	4114	KLSRV_HOST_STATUS_WARNING	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Ескерту* күйі тағайындалса туындайды. Сіз шарттарды конфигурациялай аласыз, оларды орындау кезінде құрылғының күйі *Ескерту* болып өзгереді.	90 күн
Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі жақын арада асырылады	4127	KLSRV_INVLICPROD_FILLED	Лицензиялық бағдарламалар тобына қосылған үшінші тарап бағдарламаларын орнату саны лицензиялық кілттің сипаттарында көрсетілген ең жоғары рұқсат етілген мәннің 90%-на жетсе, осы типтегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Егер үшінші тарап бағдарламасы басқарылатын құрылғыларда қолданылмаса, бағдарламаны сол құрылғылардан жойыңыз. • Жақын арада үшінші тарап бағдарламасына арналған орнату саны рұқсат етілген шектен асады деп күтсеңіз, көптеген құрылғыларға үшінші тарап бағдарламасының лицензиясын алу мүмкіндігін алдын ала қарастырыңыз. Лицензиялы бағдарламалар тобының функционалдылығын қолдана отырып, лицензиялы бағдарламалардың лицензиялық кілттерін басқара аласыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Сертификат сұралды	4133	KLSRV_CERTIFICATE_REQUESTED	Ұялы құрылғыларды басқару үшін сертификатты автоматты түрде қайта шығару мүмкін болмаса, осы түрдегі оқиғалар туындайды. Төменде оқиғалардың ықтимал себептері және оқиғаға жауап беру бойынша тиісті әрекеттер берілген: • Автоматты түрде қайта шығару, **Мүмкін болса, сертификатты автоматты түрде қайта шығару** параметрі өшірілген сертификат үшін басталды. Бұл жағдай, сертификат жасау кезінде пайда болған қатеге байланысты болуы мүмкін. Сертификатты қолмен қайта шығару қажет болуы мүмкін. • Егер сіз жалпыға ортақ инфрақұрылымымен біріктіруді қолдансаңыз, оның себебі PKI-мен біріктіру және сертификат шығару үшін қолданылатын есептік жазбаның SAM-Account-Name атрибутының болмауына байланысты болуы мүмкін. Есептік жазба сипаттарын қарап шығыңыз.	90 күн
Сертификат жойылды	4134	KLSRV_CERTIFICATE_REMOVED	Егер әкімші Ұялы құрылғыларды басқару үшін кез келген түрдегі сертификатты (жалпы, пошталық, VPN) жойса, осы түрдегі оқиғалар туындайды. Сертификат жойылғаннан кейін, осы сертификатқа қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды. Бұл оқиға Ұялы құрылғыларды басқаруға қатысты ақауларды зерттеуде пайдалы болуы мүмкін.	90 күн
Сертификаттың мерзімі өтеді	6128	ServerCertificateExpiresSoon	Осы түрдегі оқиғалар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару сервері сертификаттарының жарамдылық мерзімі аяқталғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	90 күн
APNs сертификатының жарамдылық мерзімі бітті	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Осы түрдегі оқиғалар, APNs сертификатының жарамдылық мерзімі бітейін деп жатқан кезде туындайды. Сізге қолмен APNs сертификатын жаңарту және оны iOS MDM серверіне орнату қажет.	Сақталмайды

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
APNs сертификатының жарамдылық мерзімі бітейін деп жатыр	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Егер APNs сертификатының жарамдылық мерзімінің аяқталуына дейін 14 күннен аз уақыт қалса, осы түрдегі оқиғалар орын алады. APNs сертификатының жарамдылық мерзімі аяқталғаннан кейін, қолмен APNs сертификатын жаңартып, оны iOS MDM серверіне орнату керек. APNs сертификатын жарамдылық мерзімі аяқталғанға дейін жаңартуды жоспарлау ұсынылады.	Сақталмайды
FCM хабарын ұялы құрылғыға жіберу сәтсіз аяқталды	4138	KLSRV_GCM_DEVICE_ERROR	Бұл түрдегі оқиғалар Ұялы құрылғыларды басқару Android операциялық жүйесі бар басқарылатын ұялы құрылғыларға қосылу үшін Firebase Cloud Messaging (FCM) пайдалануға конфигурацияланған болса, ал FCM сервері Басқару серверінен алынған кейбір сұрауларды өңдей алмаса туындайды. Бұл дегеніміз, кейбір басқарылатын ұялы құрылғылар push хабарландыруын алмайды. Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз. FCM серверінен алынған HTTP кодтары және олармен байланысты қателер туралы қосымша ақпарат Firebase қызметінің құжаттамасында бар ("Downstream message error response codes" тарауын қараңыз).	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
FCM хабарын FCM серверіне жіберу кезінде туындаған HTTP қатесі	4139	KLSRV_GCM_HTTP_ERROR	Бұл түрдегі оқиғалар Ұялы құрылғыларды басқару Android операциялық жүйесімен басқарылатын мобильді құрылғыларды қосу үшін Firebase Cloud Messaging (FCM) пайдалануға конфигурацияланған болса және FCM сервері 200 (OK) емес HTTP коды бар Басқару серверіне салынған сұрауды қайтарса туындайды. Төменде оқиғалардың ықтимал себептері және оқиғаға жауап беру бойынша тиісті әрекеттер берілген: • FCM серверінің жағындағы мәселелер. Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз. FCM серверінен алынған HTTP кодтары және олармен байланысты қателер туралы қосымша ақпарат Firebase қызметінің құжаттамасында бар ("Downstream message error response codes" тарауын қараңыз). • Прокси-сервер жағындағы мәселелер (прокси-серверді қолдансаңыз). Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз.	90 күн
FCM хабарын FCM серверіне жіберу сәтсіз аяқталды	4140	KLSRV_GCM_GENERAL_ERROR	Бұл түрдегі оқиғалар Firebase Cloud Messaging атты HTTP протоколымен жұмыс істеу кезінде Басқару сервері жағындағы күтпеген қателерден туындайды. Оқиғаның сипаттамасындағы ақпаратты оқып, оларға тиісінше ден қойыңыз. Егер сіз мәселенің шешімін өзіңіз таба алмасаңыз, Kaspersky Техникалық қолдау қызметіне хабарласуды ұсынамыз.	90 күн
Қатты дискіде бос орын аз	4105	KLSRV_NO_SPACE_ON_VOLUMES	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғыда диск кеңістігі таусылуға жақын қалған жағдайда туындайды. Құрылғыдағы диск кеңістігін босатыңыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Басқару серверінің дерекқорында бос орын аз	4106	KLSRV_NO_SPACE_IN_DATABASE	Бұл түрдегі оқиғалар Басқару сервері дерекқорында бос орын шектеулі болған жағдайда орын алады. Егер сіз бұл мәселені шешпесеңіз, көп ұзамай Басқару сервері дерекқоры өзінің сыйымдылығына жетеді және Басқару сервері жұмыс істемей қалады. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиғаға ден қоюдың тиісті тәсілдері келтірілген. Сіз SQL Server Express Edition қолданасыз: • SQL Server Express құжаттамасында, қолданылатын нұсқа үшін дерекқор өлшеміне қойылған шектеуді тексеріңіз. Басқару серверіңіздің дерекқоры дерекқор өлшемінің шегіне жеткен болса керек. • Басқару серверінің дерекқорында сақталатын оқиғалар санын шектеңіз. • Басқару сервері дерекқорында бағдарламаларды басқару құрамдасы жіберген оқиғалар өте көп. Басқару серверінің дерекқорында Бағдарламаларды басқару құрамдасының оқиғаларын сақтауға қатысты Kaspersky Endpoint Security for Windows саясатының параметрлерін өзгертуге болады. SQL Server Express Edition жүйесінен ерекшеленетін ДҚБЖ қолданасаңыз: • Басқару серверінің дерекқорында сақталатын оқиғалар санын шектемеңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	90 күн
Қосалқы Басқару серверімен байланыс үзілді	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Бұл түрдегі оқиғалар қосалқы Басқару серверімен байланыс үзілген кезде пайда болады. Қосалқы Басқару сервері орнатылған құрылғыдағы Kaspersky Event журналын оқып, соған сәйкес әрекет етіңіз.	90 күн
Негізгі Басқару серверімен байланыс үзілді	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Бұл түрдегі оқиғалар негізгі Басқару серверімен байланыс үзілген кезде пайда болады. Негізгі Басқару сервері орнатылған құрылғыдағы Kaspersky Event журналын оқып, соған сәйкес әрекет етіңіз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Kaspersky қолданбасы модульдерінің жаңа жаңартулары тіркелді	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Бұл түрдегі оқиғалар, Басқару сервері, орнатуды мақұлдауды қажет ететін басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының жаңа жаңартуларын тіркеген жағдайда орын алады. Басқару консолі немесе Kaspersky Security Center Web Console арқылы жаңартуларды растаңыз немесе қабылдамаңыз.	90 күн
Дерекқордағы оқиғалар санының шектеуі асырылды, оқиғаларды жою басталған	4145	KLSRV_EVP_DB_TRUNCATING	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорынан ескі оқиғаларды жою, Басқару сервері дерекқорында сақталатын оқиғалардың максималды санына жеткеннен кейін басталған жағдайда орын алады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды санын көрсетіңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз.	Сақталмайды
Дерекқордағы оқиғалар санының шектеуі асырылды, оқиғалар жойылған	4146	KLSRV_EVP_DB_TRUNCATED	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорында сақталатын оқиғалардың максималды санына жеткеннен кейін Басқару сервері дерекқорынан ескі оқиғаларды жойылған жағдайда орын алады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды рұқсат етілген санын көрсетіңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз.	Сақталмайды
Аудит (SIEM серверімен байланысты сынау сәтсіз аяқталды)	5120	KLAUD_EV_SIEM_TEST_FAILED	Бұл түрдегі оқиғалар SIEM серверіне қосылу сынағы сәтсіз аяқталған кезде туындайды.	30 күн
Сертификатты автоматты түрде беру мүмкін болмады		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Бұл оқиға мобильдік құрылғы (мобильдік протокол бойынша жұмыс істейтін құрылғы) үшін клиент сертификатын жасау қатесі болған жағдайда орын алады.	90 күн

Басқару серверінің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі	Пікір
Лицензиялық кілттің 90%-дан көп бөлігі қолданылып қойған	4097	KLSRV_EV_LICENSE_CHECK_90	30 күн	
Жаңа құрылғы анықталды	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 күн	
Құрылғы топқа автоматты түрде қосылды	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 күн	
Құрылғы ереже арқылы автоматты түрде жылжытылды	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 күн	
Құрылғы топтан жойылды: желіде ұзақ уақыт бойы белсенді емес	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 күн	
Лицензиялы бағдарламалар топтарының біреуі үшін рұқсат етілген орнатулардың саны (95%-дан) асты	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 күн	
Kaspersky талдауға жіберетін файлдар пайда болды	4131	KLSRV_APS_FILE_APPEARED	30 күн	
Осы ұялы құрылғыда FCM үлгісінің идентификаторы өзгертілді	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 күн	
Жаңартулар белгіленген қалтаға сәтті көшірілді	4122	KLSRV_UPD_REPL_OK	30 күн	
Қосалқы Басқару серверімен байланыс орнатылды	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 күн	
Негізгі Басқару серверімен байланыс орнатылды	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 күн	
Дерекқорлар жаңартылды	4144	KLSRV_UPD_BASES_UPDATED	30 күн	
Аудит: Басқару серверіне қосылым орнатылды	4147	KLAUD_EV_SERVERCONNECT	30 күн	
Аудит: нысан өзгертілді	4148	KLAUD_EV_OBJECTMODIFY	30 күн	Бұл оқиға келесі нысандардағы өзгерістерді қадағалайды: • Басқару тобы • Қауіпсіздік тобы • Пайдаланушы • Орнату пакеттері • Тапсырма • Саясат • Сервер • Виртуалды сервер

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі	Пікір
Аудит: нысан күйі өзгертілді	4150	KLAUD_EV_TASK_STATE_CHANGED	30 күн	Мысалы, тапсырма қатемен аяқталса, бұл оқиға туындайды.
Аудит: топ параметрлері өзгертілді	4149	KLAUD_EV_ADMGROUP_CHANGED	30 күн	
Аудит: Басқару серверіне қосылу тоқтатылды	4151	KLAUD_EV_SERVERDISCONNECT	30 күн	
Аудит: Нысанның сипаттары өзгертілді	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 күн	Бұл оқиға келесі параметрлердегі өзгерістерді қадағалайды: • Пайдаланушы • Лицензия • Сервер • Виртуалды сервер
Аудит: Пайдаланушы рұқсаттары өзгертілді	4153	KLAUD_EV_OBJECTACLMODIFIED	30 күн	
Аудит: Басқару серверінен импортталған немесе экспортталған шифрлау кілттері	5100	KLAUD_EV_DPEKEYSEXPORT	30 күн	
Аудит (SIEM серверімен байланысты сынау сәтті аяқталды)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 күн	Бұл оқиға SIEM серверінің қосылымы сәтті орнатылған кезде пайда болады.
Резервтік сертификат жасалды		ServerReserveCertificateCreated	30 күн	Бұл оқиға басқару серверінің сертификаты жасалған кезде пайда болады.
Сертификат мерзімін ұзарту		ServerCertificateRenewed	30 күн	Бұл оқиға басқару серверінің сертификаты жаңартылған кезде орын алады.
Сертификат автоматты түрде сәтті берілді		KLSRV_CERTIFICATE_AUTO_ISSUED	30 күн	Бұл оқиға мобильдік құрылғы (мобильдік протокол бойынша жұмыс істейтін құрылғы) үшін сертификат сәтті жасалған кезде орын алады.

Резервтік сертификат жасалды, **Сертификат мерзімін ұзарту** және **Сертификат автоматты түрде сәтті берілді** оқиғаларына сәйкес келетін операциялар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару серверінің сертификаттары үшін орындалғанда ғана, осы оқиғалар басқару сервері арқылы автоматты түрде жарияланады және басқару консолінде көрсетіледі.

Желілік агент оқиғалары

Бұл бөлімде Желілік агент оқиғалары туралы ақпарат бар.

Желілік агенттің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center Желілік агентінің оқиға түрлері келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Жаңартуды орнату қатесі	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Осындай түрдегі оқиғалар, Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату сәтсіз аяқталған кезде туындайды. Оқиға, Kaspersky басқарылатын бағдарламаларының жаңартуларына жатпайды. Оқиғаның сипаттамасын оқыңыз. Бұл оқиғаның себебі, Басқару серверіндегі Windows операциялық жүйесінің мәселесі болуы мүмкін. Егер сипаттамада Windows конфигурациясының қандай да бір мәселесі туралы айтылса, бұл мәселені шешіңіз.	30 күн
Үшінші тарап бағдарламалық жасақтамасы жаңартуын орнату сәтсіз болды	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Осындай түрдегі оқиғалар, Осалдықтар мен патчтарды басқару және Ұялы құрылғыларды басқару мүмкіндіктері қолданылып жатса және үшінші тарап өндірушілерінің бағдарламалық жасақтамасын жаңарту сәтсіз аяқталған болса туындайды. Үшінші тарап бағдарламасына келтірілген сілтеменің дұрыс екенін тексеріңіз. Оқиғаның сипаттамасын оқыңыз.	30 күн
Windows Update жаңартуларын орнату сәтсіз аяқталды	7717	KLNAG_EV_WUA_INSTALL_ERROR	Осындай түрдегі оқиғалар, егер Windows Update жаңартулары сәтсіз аяқталған болса туындайды. Microsoft Windows жаңартуларын Желілік агент саясатында конфигурациялаңыз. Оқиғаның сипаттамасын оқыңыз. Microsoft білім қорындағы қатенің сипаттамасын іздеп көріңіз. Егер сіз мәселені өзіңіз шеше алмасаңыз, Microsoft техникалық қолдау қызметіне хабарласыңыз.	30 күн
Пайдаланушыларды басқару: қателер	7723	KLNAG_EV_USR_MNG_ERR	Жалпы ескерту оқиғасы.	30 күн
Sudoers файлын сілтемелік мәнге қалпына келтіру сәтсіз аяқталды	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Оқиға sudoers файлын ауыстыру қатесінің сипаттамасын қамтиды.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Түбірлік сертификаттарды орнату сәтсіз аяқталды	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Оқиға сертификаттарды орнату қатесінің сипаттамасын қамтиды.	30 күн
Түбірлік сертификаттарды өшіру сәтсіз аяқталды	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Оқиға сертификаттарды жою қатесінің сипаттамасын қамтиды.	30 күн

Желілік агенттің ескертулері оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center Желілік агентінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің ескертулері оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бағдарламалық модуль жаңартуын орнату кезінде ескерту пайда болды	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату ескертумен аяқталды	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату кейінге қалдырылды	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 күн
Қауіпсіздік мәселесі пайда болды	549	GNRL_EV_APP_INCIDENT_OCCURED	30 күн
KSN Проксиі іске қосылды. KSN қолжетімділігін тексеру сәтсіз аяқталды	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 күн
Пайдаланушыларды басқару: ескертулер	7722	KLNAG_EV_USR_MNG_WRN	30 күн
Табылған sudoers файлы сілтемелік мәнге сәйкес келмейді	7724	KLNAG_EV_SUDOER_DIFFERENT	30 күн

Желілік агенттің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center Желілік агентінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бағдарламалық модульдерінің жаңартуы сәтті орнатылды	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 күн
Бағдарламалық модуль жаңартуын орнату басталды	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бағдарлама орнатылды	7703	KLNAG_EV_INV_APP_INSTALLED	30 күн
Бағдарлама жойылды	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 күн
Бақыланатын бағдарлама орнатылды	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 күн
Бақыланатын бағдарлама жойылды	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 күн
Үшінші тарап бағдарламасы орнатылды	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 күн
Жаңа құрылғы қосылды	7708	KLNAG_EV_DEVICE_ARRIVAL	30 күн
Құрылғы жойылды	7709	KLNAG_EV_DEVICE_REMOVE	30 күн
Жаңа құрылғы анықталды	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 күн
Құрылғы авторизацияланды	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: файл оқылды	7712	KLUSRLOG_EV_FILE_READ	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: файл өзгертілді	7713	KLUSRLOG_EV_FILE_MODIFIED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: бағдарлама іске қосылды	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: басталды	7715	KLUSRLOG_EV_WDS_BEGIN	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: тоқтатылды	7716	KLUSRLOG_EV_WDS_END	30 күн
Үшінші тарап бағдарламалық жасақтамасының жаңартуы сәтті орнатылды	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату басталды	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 күн
KSN Проксиі іске қосылды. KSN қолжетімділігін тексеру сәтті аяқталды	7719	KSNPROXY_STARTED_CON_CHK_OK	30 күн
KSN Проксиі тоқтатылды	7720	KSNPROXY_STOPPED	30 күн

iOS MDM сервері оқиғалары

Бұл бөлімде iOS MDM сервері оқиғалары туралы ақпарат бар.

iOS MDM серверінің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center iOS MDM серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

iOS MDM серверінің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Профильдер тізімін сұрау мүмкін болмады	PROFILELIST_COMMAND_FAILED	30 күн
Профильді орнату мүмкін болмады	INSTALLPROFILE_COMMAND_FAILED	30 күн
Профильді жою мүмкін болмады	REMOVEPROFILE_COMMAND_FAILED	30 күн
Provisioning профильдерінің тізімін сұрау мүмкін болмады	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 күн
Provisioning профилін орнату мүмкін болмады	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 күн
Provisioning профилін жою мүмкін болмады	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 күн
Цифрлық сертификаттардың тізімін сұрау мүмкін болмады	CERTIFICATELIST_COMMAND_FAILED	30 күн
Орнатылған бағдарламалар тізімін сұрау мүмкін болмады	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 күн
Ұялы құрылғы туралы жалпы ақпаратты сұрау мүмкін болмады	DEVICEINFORMATION_COMMAND_FAILED	30 күн
Қауіпсіздік туралы ақпаратты сұрау мүмкін болмады	SECURITYINFO_COMMAND_FAILED	30 күн
Ұялы құрылғыны бұғаттау мүмкін болмады	DEVICELOCK_COMMAND_FAILED	30 күн
Құпиясөзді тазалау мүмкін болмады	CLEARPASSCODE_COMMAND_FAILED	30 күн
Ұялы құрылғының деректерін жою мүмкін болмады	ERASEDEVICE_COMMAND_FAILED	30 күн
Қосымшаны орнату мүмкін болмады	INSTALLAPPLICATION_COMMAND_FAILED	30 күн
Қосымша үшін өтеу кодын орнату мүмкін болмады	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 күн
Басқарылатын бағдарламалар тізімін сұрау мүмкін болмады	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 күн
Басқарылатын қосымшаны жою мүмкін болмады	REMOVEAPPLICATION_COMMAND_FAILED	30 күн
Роуминг параметрлері қабылданбады	SETROAMINGSETTINGS_COMMAND_FAILED	30 күн
Қолданба жұмысында қате пайда болды	PRODUCT_FAILURE	30 күн
Пәрменді орындау нәтижесі дұрыс емес деректерді қамтиды	MALFORMED_COMMAND	30 күн
Push-хабарландыруды жіберу сәтсіз болды (Push Notification)	SEND_PUSH_NOTIFICATION_FAILED	30 күн
Пәрменді жіберу мүмкін болмады	SEND_COMMAND_FAILED	30 күн
Құрылғы табылмады	DEVICE_NOT_FOUND	30 күн

iOS MDM серверінің ескерту оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center iOS MDM серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

iOS MDM серверінің ескерту оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бұғатталған ұялы құрылғыны қосу әрекеті	INACTICE_DEVICE_TRY_CONNECTED	30 күн
Профильді жою	MDM_PROFILE_WAS_REMOVED	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Клиенттік сертификатты қайтадан пайдалану әрекеті	CLIENT_CERT_ALREADY_IN_USE	30 күн
Белсенді емес құрылғы анықталды	FOUND_INACTIVE_DEVICE	30 күн
Өтеу коды керек	NEED_REDEMPTION_CODE	30 күн
Профиль құрылғыдан жойылған саясатқа қосылды	UMDM_PROFILE_WAS_REMOVED	30 күн

iOS MDM серверінің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center iOS MDM серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

iOS MDM серверінің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Жаңа ұялы құрылғы қосылды	NEW_DEVICE_CONNECTED	30 күн
Профильдер тізімін сұрау сәтті орындалды	PROFILELIST_COMMAND_SUCCESSFULL	30 күн
Профильді орнату сәтті орындалды	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 күн
Профильді жою сәтті орындалды	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 күн
Provisioning профильдерінің тізімін сұрау сәтті орындалды	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 күн
Provisioning профилін орнату сәтті орындалды	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 күн
Provisioning профилін жою сәтті орындалды	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 күн
Цифрлық сертификаттардың тізімін сұрау сәтті орындалды	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 күн
Орнатылған бағдарламалар тізімін сұрау сәтті орындалды	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 күн
Ұялы құрылғы туралы жалпы ақпаратты сұрау сәтті орындалды	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 күн
Қауіпсіздік туралы ақпаратты сұрау сәтті орындалды	SECURITYINFO_COMMAND_SUCCESSFULL	30 күн
Ұялы құрылғы сәтті бұғатталды	DEVICELOCK_COMMAND_SUCCESSFULL	30 күн
Құпиясөзді тазалау сәтті орындалды	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 күн
Деректер ұялы құрылғыдан жойылды	ERASEDEVICE_COMMAND_SUCCESSFULL	30 күн
Қосымшаны орнату сәтті орындалды	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 күн
Қосымша үшін өтеу кодын орнату сәтті өтті	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 күн
Басқарылатын бағдарламалар тізімін сұрау сәтті орындалды	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 күн
Басқарылатын қолданба сәтті жойылды	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 күн
Роуминг параметрлері сәтті қолданылды	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 күн

Жиі болатын оқиғаларды бұғаттау

Бұл бөлімде жиі болатын оқиғалар туралы ақпарат, жиі болатын оқиғалардың бұғатталуын болдырмау, жиі болатын оқиғалар тізімін файлға экспорттау туралы ақпарат келтірілген.

Жиі болатын оқиғаларды бұғаттау туралы

Бір немесе бірнеше басқарылатын құрылғыларда орнатылған Kaspersky Endpoint Security for Windows сияқты басқарылатын бағдарлама Басқару серверіне көптеген бір тіпті оқиғаларды жібере алады. Жиі болатын оқиғаларды қабылдау Басқару сервері дерекқорының шамадан тыс жүктелуіне және басқа оқиғалардың қайта жазылуына әкелуі мүмкін. Басқару сервері барлық алынған оқиғалар саны дерекқор үшін белгіленген шектен асқан кезде ең жиі болатын оқиғаларды бұғаттай бастайды.

Басқару сервері жиі болатын оқиғаларды автоматты түрде бұғаттайды. Сіз жиі болатын оқиғаларды өзіңіз бұғаттай алмайсыз немесе қандай оқиғаларды бұғаттауды таңдай алмайсыз.

Бұғатталған оқиғаларды **Жиі болатын оқиғаларды бұғаттау** бөліміндегі Басқару сервері сипаттарынан тексеруге болады. Егер оқиға бұғатталған болса, келесі әрекеттерді орындауға болады:

- Дерекқордың қайта жазылуына жол бергіңіз келмесе, оқиғалардың осы түрін алуға тыйым салуды жалғастыра аласыз.
- Егер сіз, мысалы, жиі болатын оқиғаларды Басқару серверіне жіберудің себебін білгіңіз келсе, сіз жиі болатын оқиғалардың құлпын ашып, кез келген жағдайда оқиғалардың осы түрін алуды жалғастыра аласыз.
- Егер сіз жиі болатын оқиғаларды қайтадан бұғатталғанға дейін жалғастырғыңыз келсе, жиі болатын оқиғаларды бұғаттауды болдырмауға болады.

Жиі болатын оқиғаларды бұғаттауды басқару

Басқару сервері жиі болатын оқиғаларды автоматты түрде бұғаттайды, бірақ сіз бұғаттаудан бас тартып, жиі хабарлар алуды жалғастыра аласыз. Сондай-ақ, бұрын құлпы ашылған жиі болатын оқиғаларды алуға тыйым салуға болады.

Жиі болатын оқиғады бұғаттуды басқару үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.
2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Жиі болатын оқиғаларды бұғаттау** бөлімін таңдаңыз.
3. **Жиі болатын оқиғаларды бұғаттау** бөлімінде:
   - Алуды бұғаттағыңыз келмейтін оқиғалар үшін **Оқиға түрі** параметрін таңдаңыз.
   - Одан әрі алғыңыз келмейтін оқиғалар үшін **Оқиға түрі** параметрін таңдауды болдырмаңыз.

4. **Қолдану** түймесін басыңыз.

5. **ОК** түймесін басыңыз.

Басқару сервері сіз **Оқиға түрі** параметрін таңдаудан бас тартқан жиі оқиғаларды алады және **Оқиға түрі** параметрін таңдаған жиі оқиғаларды алуға тыйым салады.

Жиі болатын оқиғады бұғаттауды болдырмау

Сіз жиі болатын оқиғаларды бұғаттаудан бас тарта аласыз және Басқару сервері жиі болатын оқиғалардың осы түрін қайтадан бұғаттағанға дейін оқиғаларды ала бастай аласыз.

Жиі болатын оқиғаларды бұғаттауды болдырмау үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Жиі болатын оқиғаларды бұғаттау** бөлімін таңдаңыз.

3. **Жиі болатын оқиғаларды бұғаттау** бөлімінде бұғаттуды болдырмағыңыз келетін жиі болатын оқиға жолын басыңыз.

4. **Жою** түймесін басыңыз.

Жиі болатын оқиға жиі болатын оқиғалар тізімінен жойылады. Басқару сервері осы түрдегі оқиғаларды алып тұрады.

Жиі болатын оқиғалар тізімін файлға экспорттау

Жиі болатын оқиғалар тізімін файлға экспорттау үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Жиі болатын оқиғаларды бұғаттау** бөлімін таңдаңыз.

3. **Файлға экспортталуда** түймесін басыңыз.

4. Ашылған **Басқаша сақтау** терезесінде тізімді сақтау қажет файл жолын көрсетіңіз.

5. **Сақтау** түймесін басыңыз.

Барлық жиі болатын оқиғалар тізімінің жазбалары файлға экспортталады.

Виртуалды машиналардың күйінің өзгеруін бақылау

Басқару сервері жабдық тізімдемесі және орнатылған бағдарламалар тізімі, басқарылатын бағдарламалар, тапсырмалар және саясаттар параметрлері сияқты басқарылатын құрылғылардың күйі туралы ақпаратты сақтайды. Егер басқарылатын құрылғы виртуалды машина болса, пайдаланушы кез келген уақытта оның күйін бұрын жасалған виртуалды машина кескінінен (snapshot) қалпына келтіре алады. Нәтижесінде, Басқару серверіндегі виртуалды машинаның күйі туралы ақпарат өзекті болмауы мүмкін.

Мысалы, әкімші басқару серверінде 12:00-де қорғаныс саясатын бастады, ол VM_1 виртуалды машинасында 12:01-де іске қосыла бастады. 12:30-да VM_1 виртуалды машинасының пайдаланушысы оны 11:00-де жасалған снапшоттан қалпына келтіру арқылы күйін өзгертті. Қорғаныс саясатының виртуалды машинада орындалуы тоқтайды. Алайда, Басқару серверінде VM_1 виртуалды машинасында қорғау саясаты әрекетін жалғастырып жатқандығы туралы өзекті емес ақпарат сақталады.

Kaspersky Security Center бағдарламасы виртуалды машиналардың күйінің өзгеруін бақылауға мүмкіндік береді.

Құрылғымен әрбір синхрондаудан кейін Басқару сервері құрылғыда да, Басқару серверінде де сақталатын бірегей идентификаторды құрайды. Келесі синхрондауды бастамас бұрын, Басқару сервері екі жақтағы идентификаторлардың мәндерін салыстырады. Егер идентификатор мәндері сәйкес келмесе, Басқару сервері виртуалды машинаны кескіннен қалпына келтірілген деп санайды. Басқару сервері осы виртуалды машина үшін қолданылатын саясат пен тапсырма параметрлерін қалпына келтіреді және оған өзекті саясаттар мен топтық тапсырмалар тізімін жібереді.

Жүйелік тізімдемедегі ақпарат арқылы антивирустық қорғаныс күйін бақылау

Құрылғының операциялық жүйесіне байланысты жүйелік тізімдемеге Желілік агент жазған ақпаратты пайдаланып, клиент құрылғысындағы антивирустық қорғаныс күйін бақылау үшін:

- Windows басқаратын құрылғыларда:

  1. Клиент құрылғысының жүйелік тізімдемесін (мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен) ашыңыз.

  2. Келесі бөлімге өтіңіз:

     - 32 разрядты жүйе үшін:
       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - 64 разрядты жүйе үшін:
       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     Нәтижесінде, жүйелік тізімдемеде клиент құрылғысының антивирустық қорғанысының күйі туралы ақпарат көрсетіледі.

- Linux басқаратын құрылғыларда:

  - Ақпарат бөлек мәтіндік файлдарда, /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/ бойынша орналасқан әрбір деректер түрі үшін бір-бірден қамтылған.

- macOS басқаратын құрылғыларда:

  - Ақпарат бөлек мәтіндік файлдарда, /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/ бойынша орналасқан әрбір деректер түрі үшін бір-бірден қамтылған.

Антивирустық қорғаныс күйі төмендегі кестеде сипатталған кілттердің мәндеріне сәйкес келеді.

Тізімдеме кілттері және олардың мүмкін мәндері

Кілт (деректер түрі)	Мән	Сипаттамасы
`Protection_LastConnected (REG_SZ)`	КК-АА-ЖЖЖЖ СС-ММ-СС	Басқару серверіне соңғы қосылу күні мен уақыты (UTC пішімінде).
`Protection_AdmServer (REG_SZ)`	IP, DNS атауы немесе NetBIOS атауы	Құрылғыны басқаратын Басқару серверінің атауы.
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Құрылғыда орнатылған Желілік агенттің жинақ нөмірі.
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (патч1; патч2; ...; патчN)	Құрылғыда орнатылған Желілік агент нұсқасының нөмірі (патчтарымен).
`Protection_HostId (REG_SZ)`	Құрылғы идентификаторы	Құрылғы идентификаторы.
`Protection_DynamicVM (REG_DWORD)`	0 – жоқ 1 – иә	Желілік агент VDI үшін динамикалық режимге орнатылған.
`Protection_AvInstalled (REG_DWORD)`	0 – жоқ 1 – иә	Қауіпсіздік бағдарламасы құрылғыға орнатылған.
`Protection_AvRunning (REG_DWORD)`	0 – жоқ 1 – иә	Құрылғыда нақты уақыт режимінде қорғау қосулы.
`Protection_HasRtp (REG_DWORD)`	0 – жоқ 1 – иә	Нақты уақыт режимінде қорғау құрамдасы орнатылған.
`Protection_RtpState (REG_DWORD)`	Нақты уақыт режимінде қорғау күйі:	
	0	Белгісіз
	1	Өшірулі
	2	Кідіртілді.
	3	Іске қосылады.
	4	Қосулы.
	5	Жоғары қорғаныс деңгейімен қосылған (ең жоғары қорғаныс).
	6	Төмен қорғаныс деңгейімен қосылған (ең жоғары жылдамдық).
	7	Әдепкі бойынша параметрлермен қосылған (ұсынылған параметрлер).
	8	Пайдаланушы параметрлерімен қосылған.
	9	Жұмыстағы ақау.
`Protection_LastFscan (REG_SZ)`	КК-АА-ЖЖЖЖ СС-ММ-СС	Соңғы рет толық сканерлеу күні мен уақыты (UTC пішімінде).
`Protection_BasesDate (REG_SZ)`	КК-АА-ЖЖЖЖ СС-ММ-СС	Бағдарлама дерекқорларын шығару күні мен уақыты (UTC пішімінде).

Құрылғы белсенді емес кезде әрекеттерді қарау және конфигурациялау

Егер басқару тобының клиент құрылғылары белсенді болмаса, сіз бұл туралы хабарландыру ала аласыз. Сондай-ақ, мұндай құрылғыларды автоматты түрде жоюға болады.

Басқару тобында құрылғылар белсенді болмаған кезде әрекеттерді көру немесе конфигурациялау үшін:

1. Қажетті басқару тобының атауын тінтуірдің оң жақ түймесімен басыңыз.
2. Мәнмәтіндік мәзірден **Сипаттар** тармағын таңдаңыз.

   Басқару тобының сипаттары терезесі ашылады.
3. **Сипаттар** терезесінде **Құрылғылар** бөліміне өтіңіз.
4. Қажет болса, келесі параметрлерді қосыңыз немесе өшіріңіз:

   - **Құрылғы мынанша (тәулік) астам белсенді емес болса, әкімшіге хабарлау**

     Егер бұл параметр қосулы болса, әкімші құрылғылардың белсенді еместігі туралы хабарландыру алады. Енгізу өрісінде сіз **Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды** оқиғасын қалыптастыратын уақыт аралығын орната аласыз. Әдепкі бойынша белгіленген уақыт аралығы – 7 күн.

     Әдепкі бойынша, параметр қосулы.

   - **Мына уақыттан көбірек белсенді емес болса, құрылғыны топтан жойыңыз (тәулік)**

     Егер бұл параметр қосулы болса, құрылғы басқару тобынан автоматты түрде жойылатын уақыт аралығын көрсетуге болады. Әдепкі бойынша белгіленген уақыт аралығы – 60 күн.

     Әдепкі бойынша, параметр қосулы.

   - **Тектік топтан иелену**

     Егер жалауша қойылса, осы бөлімдегі параметрлер клиент құрылғысы кіретін тектік топтан иеленетін болады. Егер жалауша қойылса, **Құрылғының желідегі белсенділігі** параметрлер блогындағы параметрлерді өзгерту мүмкін емес.

     Бұл параметр тектік басқару тобы бар басқару тобы үшін ғана қолжетімді.

     Әдепкі бойынша, параметр қосулы.

   - **Еншілес топтарда мәжбүрлеп иелену**

     Параметрлер мәндері еншілес топтарға бөлінеді, бірақ еншілес топтардың сипаттарында бұл параметрлер өзгертулер үшін қолжетімді емес.

     Әдепкі бойынша, параметр өшірулі.
5. **OK** түймесін басыңыз.

Сіздің өзгертулеріңіз сақталды және қолданылды.

Kaspersky хабарландыруларын өшіру

Kaspersky Security Center Web Console бағдарламасында, Kaspersky хабарландырулары бөлімі (**Бақылау және есеп беру → Kaspersky хабарландырулары**) Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын бағдарламалар туралы ақпаратты ұсынады. Kaspersky хабарландыруларын алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

Kaspersky хабарландырулары екі түрлі ақпаратты қамтиды: қауіпсіздікке қатысты хабарландырулар және жарнамалық хабарландырулар. Сіз әрбір түрдегі хабарландыруларды бөлек өшіре аласыз.

Қауіпсіздікпен байланысты хабарландыруларды өшіру үшін:

1. Консоль ағашында қауіпсіздікке қатысты хабарландыруларды өшіру үшін Басқару серверін таңдаңыз.
2. Нысанның контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттарының ашылған терезесінде, **Kaspersky хабарландырулары** бөлімінде **Kaspersky Security Center Web Console консолінде Kaspersky хабарландырулары дисплейін қосу** нұсқасын таңдаңыз.
4. **OK** түймесін басыңыз.

Kaspersky хабарландырулары өшірулі.

Жарнамалық хабарландырулар әдепкі бойынша өшірулі. Сіз Kaspersky Security Network (KSN) қосқан жағдайда ғана жарнамалық хабарландырулар аласыз. KSN өшіру арқылы хабарландырулардың бұл түрін өшіруге болады.

Тарату нүктелері мен қосылым шлюздерін конфигурациялау

Kaspersky Security Center-дегі басқару топтарының құрылымы келесі функцияларды орындайды:

- Саясаттардың әрекет ету ауқымын белгілеу.

  Саясат профильдерінің көмегімен құрылғыларда параметрлердің сыртқы жиынтықтарын қолданудың баламалы тәсілі бар. Бұл жағдайда, саясаттардың әрекет ету ауқымы тегтер, құрылғылардың Active Directory ұйымдық бөлімшесінде орналасқан жерлері, Active Directory қауіпсіздік топтарындағы мүшелік және т.б. арқылы белгіленеді.

- Топтық тапсырмалардың әрекет ету ауқымын белгілеу.

  Басқару топтарының иерархиясына негізделмеген топтық тапсырмалардың әрекет ету ауқымын белгілеу тәсілдемесі бар: құрылғыларды таңдау және арнайы құрылғылар үшін тапсырмаларды қолдану.

- Құрылғыларға, виртуалды және қосалқы Басқару серверлеріне қатынасу құқықтарын белгілеу.

- Тарату нүктелерін тағайындау.

Басқару топтарының құрылымын құру кезінде тарату нүктелерін оңтайлы түрде тағайындау үшін ұйым желісінің топологиясын ескеру қажет. Тарату нүктелерінің оңтайлы таралуы арқасында ұйым желісіндегі желілік трафикті азайтуға мүмкіндік беріледі.

Ұйымның ұйымдық құрылымына және желілер топологиясына байланысты, басқару топтары құрылымының келесі типтік конфигурацияларын ажыратуға болады:

- Бір кеңсе
- Көптеген шағын оқшауланған кеңселер

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Тарату нүктелерінің типтік конфигурациясы: бір кеңсе

"Бір кеңсе" типтік конфигурациясында барлық құрылғылар ұйымның желісінде орналаса отырып, бір-бірін "көреді". Ұйымның желісі тар арналармен байланысқан бірнеше бөлектенген бөліктен (желіден немесе желі сегменттерінен) құралуы мүмкін.

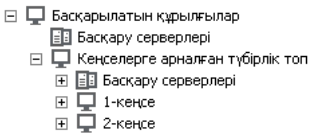
Басқару топтарының құрылымын құрудың келесі тәсілдері болуы мүмкін:

- Желі топологиясын ескере отырып, басқару тобының құрылымын құру. Басқару топтарының құрылымы желінің топологиясын нақты түрде көрсетуге міндетті емес. Желінің бөлектенген бөліктеріне қандай да бір басқару топтарының сай келуі жеткілікті. Тарату нүктелерін автоматты түрде тағайындауды қолдануға немесе тарату нүктелерін қолмен тағайындауға болады.
- Желінің топологиясын білдірмейтін басқару топтарының құрылымын құру. Бұл жағдайда, тарату нүктелерін автоматты түрде тағайындауды өшіру және желінің әрбір бөлектенген бөлігінде түбірлік басқару тобына, мысалы, **Басқарылатын құрылғылар** тобына бір немесе бірнеше құрылғыны тарату нүктелері ретінде тағайындау керек. Барлық тарату нүктелері бір деңгейде болады және бірдей "ұйым желісінің барлық құрылғылары" әрекет ету ауқымына ие болады. Желілік агенттердің әрқайсысы, бағыты ең қысқа болып саналатын тарату нүктесіне қосылатын болады. Тарату нүктесіне апаратын бағытты tracert утилитасының көмегімен анықтауға болады.

Тарату нүктелерінің типтік конфигурациясы: қашықтағы көптеген шағын кеңселер

Бұл типтік конфигурация, бәлкім, басты кеңсемен интернет арқылы байланысқан көптеген шағын қашықтағы кеңселерге сәйкес келеді. Қашықтағы кеңселердің әрқайсысы NAT артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес – кеңселер бір-бірінен оқшауланған.

Конфигурация басқару топтарының құрылымында міндетті түрде көрсетілуі керек: қашықтағы кеңселердің әрқайсысы үшін жеке басқару тобын құру керек (төмендегі суреттегі **1-кеңсе**, **2-кеңсе** топтары).



Қашықтағы кеңселер басқару топтарының құрылымында көрсетілген

Кеңсеге сай келетін әрбір басқару тобына бір немесе бірнеше тарату нүктесін тағайындау керек. Дискіде жеткілікті орны бар қашықтағы кеңсе құрылғыларын тарату нүктелері ретінде тағайындау керек. Мысалы, **1-кеңсе** тобында орналастырылған құрылғылар **1-кеңсе** басқару тобына тағайындалған тарату нүктелеріне жүгінетін болады.

Егер кейбір пайдаланушылар ноутбуктері бар кеңселер арасында физикалық түрде жылжытылатын болса, әр қашықтағы кеңседе жоғарыда аталған тарату нүктелеріне тағы екі және немесе одан да көп құрылғыны таңдап, оларды жоғарғы деңгейдегі басқару тобына тарату нүктелері ретінде тағайындау керек (жоғарыдағы суреттегі **Кеңселерге арналған түбірлік топ** тобы).

1-кеңсе басқару тобында болған, бірақ физикалық түрде **2-кеңсе** тобына сәйкес келетін кеңсеге көшірілген ноутбук. Жылжытқаннан кейін, ноутбуктағы Желілік агент **1-кеңсе** тобына тағайындалған тарату нүктелеріне жүгінуге тырысатын болады, бірақ бұл тарату нүктелері қолжетімді болмайды. Сонда Желілік агент **Кеңселерге арналған түбірлік топ** тобына тағайындалған тарату нүктелеріне жүгіне бастайды. Қашықтағы кеңселер бір-бірінен алшақ орналасқандықтан, **Кеңселерге арналған түбірлік топ** басқару тобына тағайындалған барлық тарату нүктелерінен **2-кеңсе** тобына тағайындалған тарату нүктелеріне жүгіну ғана сәтті болады. Яғни, ноутбук өзінің бастапқы кеңсесіне сәйкес келетін басқару тобында бола отырып, қазіргі уақытта физикалық түрде орналасқан кеңсенің тарату нүктесін қолдана беретін болады.

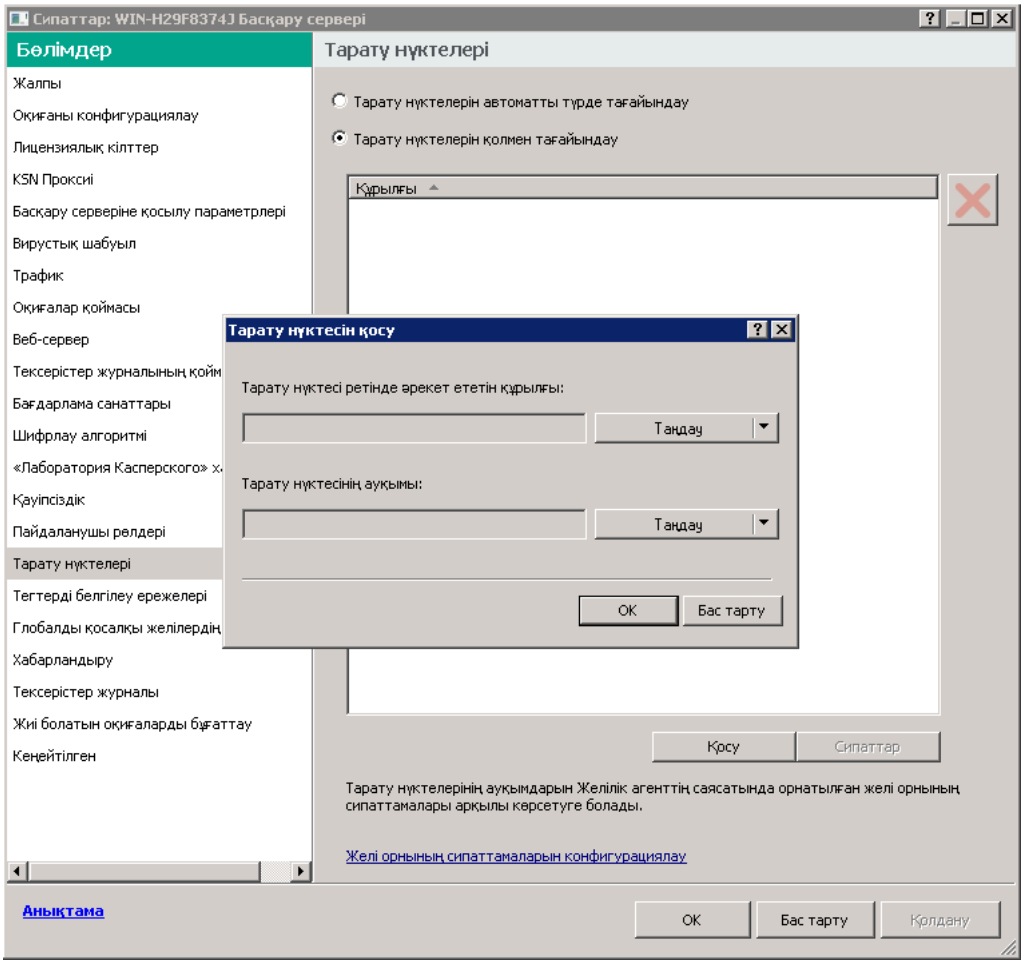
Басқарылатын құрылғыны тарату нүктесі етіп тағайындау

Құрылғыны басқару тобына тарату нүктесі ретінде қолмен тағайындауға және оны Басқару консоліндегі қосылым шлюзі ретінде конфигурациялауға болады.

Құрылғыны басқару тобының тарату нүктесі ретінде тағайындау үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде **Тарату нүктелері** бөлімін таңдаңыз.
4. Терезенің оң жағында **Тарату нүктелерін қолмен тағайындау** параметрін таңдаңыз.

5. **Қосу** түймесін басыңыз.



Тарату нүктесін қолмен тағайындау

Тарату нүктесін қосу терезесі ашылады.

6. **Тарату нүктесін қосу** терезесінде келесі әрекеттерді орындаңыз:

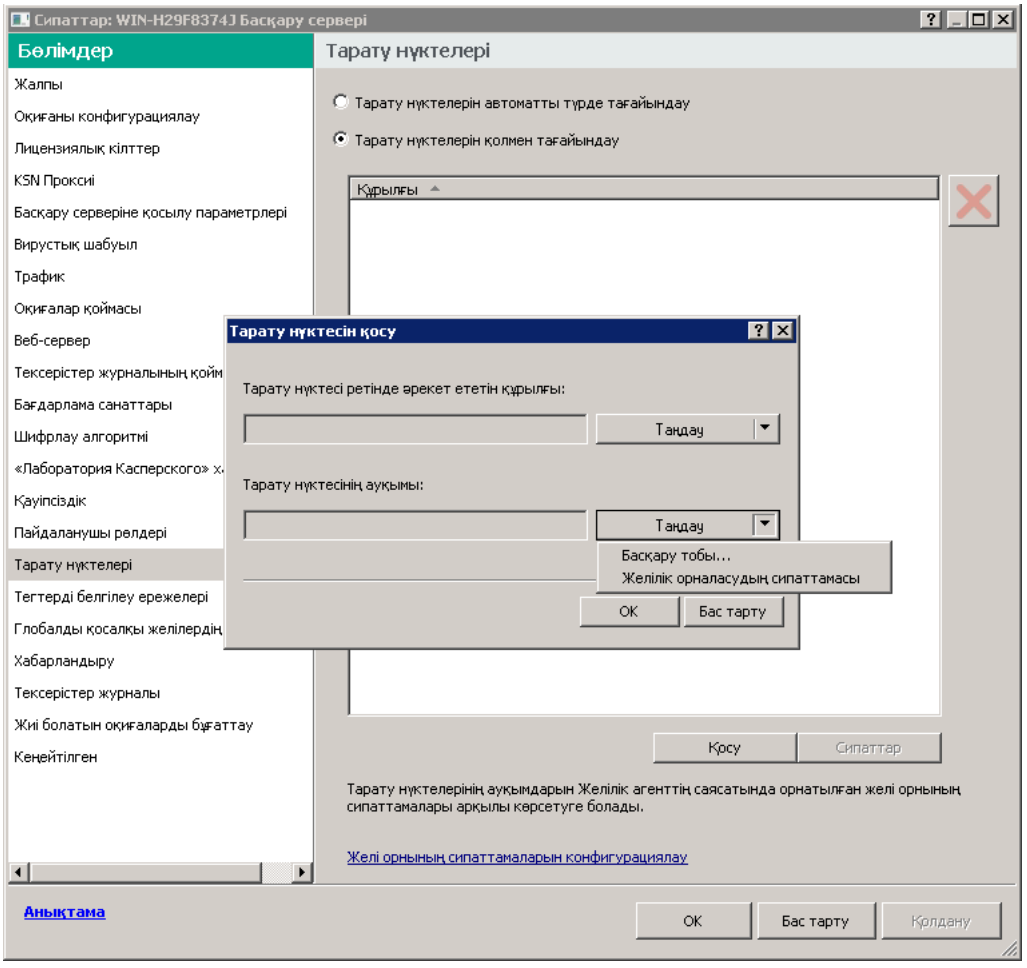
   a. **Тарату нүктесі ретінде әрекет ететін құрылғы** бөлімінде **Таңдау** түймесінің жанындағы төмен (▾) нұсқасын басып, **Мына топтан құрылғы қосу** нұсқасын таңдаңыз.

   b. Ашылып жатқан **Құрылғыларды таңдау** терезесінде тарату нүктесі ретінде әрекет ететін құрылғыны таңдаңыз.

   c. **Тарату нүктесінің ауқымы** бөлімінде **Таңдау** ашылмалы түймесінің жанындағы төмен (▾) нұсқасын басыңыз.

d. Тарату нүктесі жаңартуларды тарататын құрылғылар жиынтығын көрсетіңіз. Басқару тобын немесе желілік орналасудың сипаттамасын көрсете аласыз.

e. **Тарату нүктесін қосу** терезесін жабу үшін **OK** түймесін басыңыз.



Тарату нүктесінің ауқымын таңдау

Қосылған тарату нүктесі **Тарату нүктелері** бөліміндегі тарату нүктелерінің тізімінде пайда болады

Виртуалды Басқару серверіне қосылатын бірінші Желілік агент орнатылған құрылғы автоматты түрде тарату нүктесі ретінде тағайындалады және қосылым шлюзі ретінде конфигурацияланады.

Linux жүйесінде жұмыс істейтін құрылғыны демилитаризацияланған аймақта шлюз ретінде қосу

Linux жүйесінде жұмыс істейтін құрылғыны демилитаризацияланған аймақта (DMZ) шлюз ретінде қосу үшін:

1. Желілік агентті жүктеп алыңыз да, Linux құрылғысына орнатыңыз.

2. Орнатудан кейінгі скриптті іске қосыңыз және жергілікті ортаның конфигурациясын реттеу үшін шебердің нұсқауларын орындаңыз. Пәрмен жолында келесі пәрменді орындаңыз:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Желілік агент режимін сұрау қадамында **Қосылым шлюзі ретінде қолдану** параметрін таңдаңыз.

4. MMC негізіндегі Басқару консолінде, Басқару сервері саясатының контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

5. Ашылған Басқару сервері сипаттары терезесінде **Тарату нүктелері** бөлімін таңдаңыз.

6. Терезенің оң жағында ашылған **Тарату нүктелері** терезесінде:

   a. **Тарату нүктелерін қолмен тағайындау** параметрін таңдаңыз.

   b. **Қосу** түймесін басыңыз.

   Тарату нүктесін қосу терезесі ашылады.

7. **Тарату нүктесін қосу** терезесінде келесі әрекеттерді орындаңыз:

   a. **Тарату нүктесі ретінде әрекет ететін құрылғы** бөлімінде **Таңдау** ашылмалы түймесінің жанындағы төмен (▾) нұсқасын басып, **Келесі мекенжай бойынша демилитаризацияланған аймақтағы қосылымдар шлюзін қосу** нұсқасын таңдаңыз.

   b. **Тарату нүктесінің ауқымы** бөлімінде **Таңдау** ашылмалы түймесінің жанындағы төмен (▾) нұсқасын басыңыз.

   c. Тарату нүктесі жаңартуларды тарататын құрылғылар жиынтығын көрсетіңіз. Сіз басқару тобын көрсете аласыз.

   d. **Тарату нүктесін қосу** терезесін жабу үшін **OK** түймесін басыңыз.

8. Қосылған тарату нүктесі **Тарату нүктелері** бөліміндегі тарату нүктелерінің тізімінде пайда болады

9. Kaspersky Security Center бағдарламасымен қосылымның сәтті түрде конфигурацияланғанын тексеру үшін klnagchk утилитасын іске қосыңыз. Пәрмен жолында келесі пәрменді енгізіңіз:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. Басты мәзірде Kaspersky Security Center бағдарламасына өтіп, құрылғыны табыңыз.

11. Пайда болған терезеде <Құрылғы атауы> түймесін басыңыз.

12. Ашылмалы тізімнен **Топқа жылжыту** сілтемесін таңдаңыз.

13. Ашылған **Топты таңдау** терезесінде **Тарату нүктелері** сілтемесінен өтіңіз.

14. **OK** түймесін басыңыз.

15. Пәрмен жолында пәрменді орындау арқылы Linux клиентінде Желілік агент қызметін қайта іске қосыңыз:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Linux жүйесінде жұмыс істейтін құрылғыны демилитаризацияланған аймақта шлюз ретінде қосу аяқталды.

Осыдан кейін, конфигурацияланған қосылым шлюзі арқылы Linux басқаруымен жұмыс істейтін құрылғыны Басқару серверіне қосуға болады. Бұл процедураларды негізгі орнату сценарийі аяқталғаннан кейін ғана орындаңыз.

Linux жүйесінде жұмыс істейтін құрылғыны қосылым шлюзі арқылы Басқару серверіне қосу

Қосылым шлюзі клиент құрылғыларын демилитаризияланған аймақтан (DMZ) Басқару серверіне қосуға мүмкіндік береді. Windows және Linux негізіндегі құрылғылар қосылым шлюзі ретінде әрекет ете алады. Қосылым шлюзін қосқаннан және конфигурациялағаннан кейін, Linux басқаруымен жұмыс істейтін құрылғыны Басқару серверіне қосу үшін осы шлюзді пайдалана аласыз. Төменде сипатталған процедураны тек негізгі орнату сценарийі аяқталғаннан кейін ғана орындаңыз.

Linux жүйесінде жұмыс істейтін құрылғыны қосылым шлюзі арқылы Басқару серверіне қосу үшін осы құрылғыда келесі әрекеттерді орындаңыз:

1. Желілік агентті жүктеп алыңыз да, Linux құрылғысына орнатыңыз.

2. Пәрмен жолында келесі пәрменді орындау арқылы Желілік агенттің орнатудан кейінгі скриптін іске қосыңыз:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Желілік агент режимін сұрайтын қадамда **Серверге байланыс шлюзі арқылы қосылу** параметрін таңдап, қосылым шлюзінің мекенжайын енгізіңіз.

4. Пәрмен жолындағы келесі пәрмен арқылы Kaspersky Security Center бағдарламасы мен қосылым шлюзі арасындағы байланысты тексеріңіз:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   Шығыс деректерінде қосылым шлюзінің мекенжайы көрсетіледі.

Linux жүйесінде жұмыс істейтін құрылғыны қосылым шлюзі арқылы Басқару серверіне қосу аяқталды. Бұл құрылғыны сіз жаңартуларды тарату, бағдарламаларды қашықтан орнату және желілік құрылғылар туралы ақпарат алу үшін пайдалана аласыз.

Қосылым шлюзін тарату нүктесі ретінде демилитаризацияланған аймаққа қосу

Қосылым шлюзі Басқару серверімен байланыс орнатпайды, тек Басқару серверінен қосылымдарды күтеді. Бұл дегеніміз, демилитаризацияланған аймақта құрылғыға қосылым шлюзін орнатқаннан кейін, Басқару сервері басқарылатын құрылғылардың арасында құрылғыны тізімдемейді. Сол себепті, Басқару сервері қосылым шлюзіне қосылуды бастау үшін сізге арнайы процедура қажет болады.

Тарату нүктесі ретінде қосылым шлюзі бар құрылғыны қосу үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.

2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесінде **Тарату нүктелері** бөлімін таңдаңыз.

4. Терезенің оң жағында **Тарату нүктелерін қолмен тағайындау** параметрін таңдаңыз.

5. **Қосу** түймесін басыңыз.

   Тарату нүктесін қосу терезесі ашылады.

6. **Тарату нүктесін қосу** терезесінде келесі әрекеттерді орындаңыз:

   a. **Тарату нүктесі ретінде әрекет ететін құрылғы** бөлімінде **Таңдау** ашылмалы түймесінің жанындағы төмен (▾) нұсқасын басып, **Байланыс шлюзін DMZ режимінде мекенжай бойынша қосу** нұсқасын таңдаңыз.

   b. Ашылған **Қосылым шлюзі мекенжайын енгізу** терезесінде қосылым шлюзінің IP мекенжайын енгізіңіз (немесе қосылым шлюзі атау бойынша қолжетімді болса, атауын енгізіңіз).

   c. **Тарату нүктесінің ауқымы** бөлімінде **Таңдау** ашылмалы түймесінің жанындағы төмен (▾) нұсқасын басыңыз.

   d. Тарату нүктесі жаңартуларды тарататын құрылғылар жиынтығын көрсетіңіз. Басқару тобын немесе желілік орналасудың сипаттамасын көрсете аласыз.

      Сыртқы басқарылатын құрылғылар үшін бөлек топ құру ұсынылады.

Осы әрекет орындалғаннан кейін, тарату нүктелерінің тізімінде **Қосылымдар шлюзі үшін уақытша жазба** атты жаңа жазбаны қамтиды.

Басқару сервері көрсетілген мекенжай бойынша қосылым шлюзіне дереу қосылуға тырысады. Бәрі сәтті өтсе, жазу атауы қосылым шлюзі құрылғысының атауына өзгереді. Бұған бес минутқа дейін уақыт кетеді.

Қосылым шлюзінің уақытша жазбасы аталған жазбаға айналғанда, қосылым шлюзі **Тағайындалмаған құрылғылар** тобында да пайда болады.

Бұған дейін конфигурацияланған желіге қосылым шлюзін қосу үшін жаңадан қосылған қосылым шлюзіне қосылғыңыз келетін құрылғыларға Желілік бағдарламасын қайта орнатыңыз.

Тарату нүктелерін автоматты түрде тағайындау

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Kaspersky Security Center бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды.

Тарату нүктелерін автоматты түрде тағайындау үшін:

1. Бағдарламаның басты терезесін ашыңыз.

2. Консоль ағашында тарату нүктелерін автоматты түрде тағайындауды қажет ететін Басқару сервері атауы бар түйінді таңдаңыз.

3. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

4. Басқару серверінің сипаттары терезесіндегі **Бөлімдер** панелінің **Тарату нүктелері** опциясын таңдаңыз.

5. Терезенің оң жағында **Тарату нүктелерін автоматты түрде тағайындау** параметрін таңдаңыз.

   Егер тарату нүктелерінің құрылғыларын автоматты түрде тағайындау қосулы болса, тарату нүктелерінің параметрлерін қолмен конфигурациялау, сондай-ақ тарату нүктелерінің тізімін өзгерту мүмкін емес.

6. **ОК** түймесін басыңыз.

   Нәтижесінде, Басқару сервері тарату нүктелерін автоматты түрде тағайындайды және олардың параметрлерін конфигурациялайды.

Тарату нүктесі таңдаған құрылғыға Желілік агентті жергілікті орнату туралы

Тарату нүктесі ретінде таңдалған құрылғы қосылым шлюзінің рөлін орындау мақсатында виртуалды Басқару серверімен тікелей байланыса алуы үшін, бұл құрылғыға Желілік агент жергілікті түрде орнатылуы керек.

Тарату нүктесі таңдаған құрылғыға Желілік агентті жергілікті орнату тәртібі кез келген желі құрылғысына Желілік агентті жергілікті орнату тәртібіне сәйкес келеді.

Тарату нүктесі таңдаған құрылғы үшін келесі шарттар орындалуы керек:

- **Басқару сервері** орнату шебері терезесінде Желілік агентті жергілікті түрде орнату барысында **Сервер мекенжайы** өрісінде құрылғыны басқаратын виртуалды Басқару серверінің мекенжайын көрсету керек. Құрылғының мекенжайы ретінде Windows желісіндегі IP мекенжайын немесе құрылғының атауын пайдалануға болады.

  Виртуалды Сервердің мекенжайын жазудың келесі нысаны қолданылады: <виртуалды Серверге бағынатын физикалық Басқару серверінің толық мекенжайы>/<Виртуалды Басқару серверінің атауы>.

- Құрылғыдағы қосылым шлюзінің рөлін орындау үшін Басқару серверімен байланысу үшін қажетті барлық порттар ашық болуы керек.

Көрсетілген параметрлері бар Желілік агентті құрылғыға орнату нәтижесінде Kaspersky Security Center бағдарламасы келесі әрекеттерді автоматты түрде орындайды:

- бұл құрылғыны виртуалды Басқару серверінің **Басқарылатын құрылғылар** тобына қосады;

- бұл құрылғыны виртуалды Басқару серверінің **Басқарылатын құрылғылар** тобының тарату нүктесі ретінде тағайындайды.

Ұйымның желісіндегі **Басқарылатын құрылғылар** тобының тарату нүктесі тағайындалған құрылғыда Желілік агентті жергілікті түрде орнатуды орындау қажет және жеткілікті. Салынған басқару топтарындағы тарату нүктелерінің рөлін атқаратын құрылғыларда Желілік агентті қашықтан орнатуға болады. Ол үшін **Басқарылатын құрылғылар** тобының таралу нүктесін қосылым шлюзі ретінде пайдаланыңыз.

Тарату нүктесін қосылым шлюзі ретінде қолдану туралы

Басқару сервері демилитаризацияланған аймақтан (DMZ) тыс болса, демилитаризацияланған аймақтағы Желілік агенттер онымен байланысу мүмкіндігін жоғалтады.

Басқару серверін Желілік агенттермен байланыстыру үшін тарату нүктесін қосылым шлюзі ретінде пайдалануға болады. Тарату нүктесі Басқару серверін қосылым жасау портын ұсынады. Іске қосу кезінде Басқару сервері тарату нүктесіне қосылады және бүкіл жұмыс уақытында онымен байланысты үзбейді.

Басқару серверінен сигнал алғаннан кейін, тарату нүктесі Желілік агенттерге UDP сигналын Басқару серверіне қосылуға жібереді. Сигнал алған кезде Желілік агенттер Желілік агент пен Басқару сервері арасындағы ақпаратты жіберетін тарату нүктесіне қосылады. Ақпарат алмасу IPv4 желісі немесе IPv6 желісі бойынша жүзеге асырылуы мүмкін.

Бөлінген құрылғыны қосылым шлюзі ретінде пайдалану және бір қосылым шлюзіне 10 000-нан аспайтын клиент құрылғыларын (ұялы құрылғыларды қоса) тағайындау ұсынылады.

Бұрын конфигурацияланған желіге қосылым шлюзін қосу үшін:

1. Желілік агентті қосылым шлюзі режимінде орнатыңыз.
2. Жаңадан қосылған қосылым шлюзіне қосқыңыз келетін құрылғыларда Желілік агентті қайта орнатыңыз.

Тарату нүктесі сұралатын ауқымдар тізіміне IP ауқымдарын қосу

IP ауқымын тарату нүктесі сұрайтын ауқымдар тізіміне қоса аласыз.

IP ауқымын сауалнамаға ауқымдары тізіміне қосу үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Басқару сервері түйінінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Ашылған Басқару сервері сипаттары терезесінде **Тарату нүктелері** бөлімін таңдаңыз.
4. Тізімнен қажетті тарату нүктесін таңдап, **Сипаттар** түймесін басыңыз.
5. **Бөлімдер** панелінде ашылған тарату нүктесі сипаттары терезесінде **Құрылғыны табу** → **IP ауқымдары** бөлімін таңдаңыз.
6. **Ауқым сауалнамасына қосу** жалаушасын қойыңыз.
7. **Қосу** түймесін басыңыз.

   Ауқым сауалнамасына қосу жалаушасы қойылса, **Қосу** белсенді болады.

   IP ауқымы терезесі ашылады.
8. **IP ауқымы** терезесінде жаңа IP ауқымы атауын енгізіңіз (әдепкі бойынша Жаңа ауқым атауы көрсетілген).

9. **Қосу** түймесін басыңыз.
10. Келесі әрекеттердің бірін орындаңыз:
    - IP ауқымын бастапқы және соңғы IP мекенжайы етіп белгілеңіз.
    - IP ауқымын мекенжай мен ішкі желі бүркеніші етіп белгілеңіз.
    - **Шолу** түймесін басып, глобалды қосалқы желілердің тізімінен ішкі желіні қосыңыз.
11. **OK** түймесін басыңыз.
12. Атауы белгіленген ауқымды қосу үшін **OK** түймесін басыңыз.

    Жаңа ауқым сауалнама ауқымдары тізімінде көрсетіледі.

Тарату нүктесін хабарлаушы сервер ретінде қолдану

Kaspersky Security Center бағдарламасында тарату нүктесі мобильді протокол арқылы басқарылатын құрылғылар үшін және Желілік агент басқаратын құрылғылар үшін push сервері ретінде жұмыс істей алады. Мысалы, егер сіз KasperskyOS орнатылған құрылғыларды Басқару серверімен мәжбүрлеп синхрондауды қосқыңыз келсе, push сервері қосулы болуы керек. Push серверінде, push сервері қосылған тарату нүктесімен бірдей басқарылатын құрылғылар аймағы бар. Егер сізде бір басқару тобына тағайындалған бірнеше тарату нүктелері болса, олардың әрқайсысында ескерту серверін қосуға болады. Бұл жағдайда, Басқару сервері жүктемені тарату нүктелері арасында бөледі.

Push сервері бір мезгілдегі 50 000 қосылымға дейінгі жүктемені қолдайды.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін тарату нүктелерін push серверлері ретінде пайдаланғыңыз келуі мүмкін. Тұрақты байланыс жергілікті тапсырмаларды іске қосу және тоқтату, басқарылатын бағдарламаның статистикасын алу немесе туннель жасау сияқты кейбір операциялар үшін қажет. Тарату нүктесін push серверінің сервері ретінде қолдансаңыз, сізге басқарылатын құрылғыларда **Басқару серверімен байланысты үзбеу** параметрін қолдану немесе Желілік агенттің UDP портына пакеттерді жіберу қажет емес.

Тарату нүктесін push сервері ретінде пайдалану үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Басқару сервері түйінінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Ашылған Басқару сервері сипаттары терезесінде **Тарату нүктелері** бөлімін таңдаңыз.
4. Тізімнен қажетті тарату нүктесін таңдап, **Сипаттар** түймесін басыңыз.
5. Тарату нүктесі сипаттарының ашылған терезесінде, **Жалпы** бөліміндегі **Бөлімдер** панелінде **Осы тарату нүктесін push-сервер ретінде пайдалану** параметрін таңдаңыз.
6. push сервері портының нөмірін, яғни клиент құрылғылары қосылу үшін пайдаланатын тарату нүктесіндегі портты көрсетіңіз.

   Әдепкі бойынша порт нөмірі – 13295.

7. Тарату нүктесі сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

8. Желілік агент саясатының сипаттары терезесін ашыңыз.

9. **Қосылым мүмкіндігі** бөлімінде **Желі** бөлікшесіне өтіңіз.

10. **Желі** бөлікшесінде **Басқару серверіне мәжбүрлі қосылу үшін тарату нүктесін пайдаланыңыз** нұсқасын таңдаңыз.

11. Терезені жабу үшін **OK** түймесін басыңыз.

    Тарату нүктесі push сервері рөлін атқара бастайды. Енді ол клиент құрылғыларына push хабарландыруларын жібере алады.

KasperskyOS операциялық жүйесі орнатылған құрылғыларды басқарсаңыз немесе мұны жасауды жоспарласаңыз, тарату нүктесін push сервері ретінде пайдалануыңыз керек. Клиент құрылғыларына push хабарландыруларын жібергіңіз келсе, тарату нүктесін push сервері ретінде пайдалануға болады.

Басқа да күнделікті тапсырмалар

Бұл бөлімде Kaspersky Security Center бағдарламасымен күнделікті жұмыс істеу бойынша ұсыныстар бар.

Басқару серверлерін басқару

Бұл бөлімде Басқару серверлерімен жұмыс істеу және Басқару сервері параметрлерін конфигурациялау туралы ақпарат бар.

Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу

Басқару серверін қосалқы Сервер ретінде қосып, осылайша "басты Сервер – қосалқы Сервер" иерархиясының қатынасын орнатуға болады. Басқару консолі арқылы қосылу үшін, қосалқы еткіңіз келетін Сервердің қолжетімді болып-болмағанына қарамастан қосуға болады.

Серверлерді иерархияға біріктіру кезінде екі Сервердің 13291-порты қолжетімді болуы керек. 13291-порт Басқару консолінен Басқару серверіне қосылымдарды қабылдау үшін керек.

Басқару серверін басты Серверге қосалқы Сервер ретінде қосу

Басқару серверін 13000-порт арқылы басты Серверге қосылатын қосалқы Сервер ретінде қосуға болады. Сізге екі Басқару серверінің TCP 13291 порттары қолжетімді болып табылатын Басқару консолі орнатылған құрылғы қажет болады:

Консоль арқылы қосылуға қолжетімді Басқару серверін қосалқы Сервер ретінде қосу үшін:

1. Қолдау көрсетілетін басты Сервердің 13000-порты қосалқы Басқару серверлерінен қосылымдарды қабылдау үшін қолжетімді екеніне көз жеткізіңіз.

2. Басқару консолін пайдаланып, болашақ негізгі Басқару серверіне қосылыңыз.

3. Қосалқы Басқару серверін қосу жоспарланып отырған басқару тобын таңдаңыз.

4. Таңдалған топтың **Басқару серверлері** түйінінің жұмыс аймағында **Қосалқы Басқару серверін қосу** сілтемесі арқылы өтіңіз.

   Қосалқы Басқару серверін қосу шебері іске қосылады.

5. Шебердің бірінші қадамында (топқа қосылған Басқару серверінің мекенжайын енгізу) болашақ қосалқы Басқару серверінің желілік атауын енгізіңіз.

6. Содан кейін, шебердің нұсқауларын орындаңыз.

"Басты Сервер – қосалқы Сервер" қатынасы орнатылады. Қосалқы Сервер басты Серверден қосылым қабылдайды.

Егер сізде екі Басқару серверінің TCP 13291 порттары қолжетімді Басқару консолі орнатылған құрылғы болмаса (мысалы, болашақ қосалқы Сервер қашықтағы кеңседе болса және қауіпсіздік мақсатында қашықтағы кеңсе жүйелік әкімшісі 13291-портты интернет арқылы қолжетімді етпесе), сіз әлі де қосалқы Серверді қоса аласыз.

Консоль арқылы қосылуға қолжетімді емес Басқару серверін қосалқы Сервер ретінде қосу үшін:

1. Болашақ басты Сервердің 13000-порты қосалқы Басқару серверлерінен қосылу үшін қолжетімді екеніне көз жеткізіңіз.

2. Болашақ негізгі Басқару сервері сертификаты файлын сыртқы құрылғыға жазыңыз (мысалы, алынбалы жетек) немесе Басқару сервері орналасқан қашықтағы кеңсенің жүйелік әкімшісіне жіберіңіз.

   Басқару сервері сертификатының файлы %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer мекенжайы бойынша Басқару серверінде орналасқан.

3. Болашақ қосалқы Басқару сервері сертификатының файлын сыртқы құрылғыға жазыңыз (мысалы, алынбалы жетек). Егер болашақ қосалқы Сервер қашықтағы кеңседе болса, қашықтағы кеңсенің жүйелік әкімшісінен сізге сертификат жіберуін сұраңыз.

   Басқару сервері сертификатының файлы %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer мекенжайы бойынша Басқару серверінде орналасқан.

4. Басқару консолін пайдаланып, болашақ негізгі Басқару серверіне қосылыңыз.

5. Қосалқы Басқару серверін қосу жоспарланып отырған басқару тобын таңдаңыз.

6. **Басқару серверлері** түйінінің жұмыс аймағындағы **Қосалқы Басқару серверін қосу** сілтемесін басыңыз.

   Қосалқы Басқару серверін қосу шебері іске қосылады.

7. Шебердің бірінші қадамында (мекенжай енгізу) **Қосалқы Басқару серверінің мекенжайы (міндетті емес)** өрісін бос қалдырыңыз.

8. **Қосалқы Басқару серверінің сертификат файлы** терезесінде **Шолу** түймесін басып, бұрын сақталған қосалқы Сервер сертификаты файлын таңдаңыз.

9. Шебердің жұмысы аяқталғаннан кейін, басқа Басқару консолі арқылы болашақ қосалқы Басқару серверіне қосылыңыз. Бұл Сервер қашықтағы кеңседе болса, қашықтағы кеңсенің жүйелік әкімшісінен болашақ қосалқы Басқару серверіне қосылуын және онда келесі қадамдарды орындауын сұраңыз.

10. **Басқару сервері** түйінінің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

11. Басқару сервері сипаттарында **Кеңейтілген** бөліміне, содан соң **Басқару серверлерінің иерархиясы** бөліміне өтіңіз.

12. **Бұл Басқару сервері иерархияда қосымша** жалаушасын қойыңыз.

    Енгізу өрістері енгізу және өңдеу үшін қолжетімді болады.

13. **Негізгі Басқару серверінің мекенжайы** өрісінде болашақ негізгі Басқару серверінің желілік атауын енгізіңіз.

14. **Шолу** түймесін басу арқылы болашақ негізгі Сервердің бұрын сақталған сертификат файлын таңдаңыз.

15. **OK** түймесін басыңыз.

"Басты Сервер – қосалқы Сервер" қатынасы орнатылады. Басқару консолі арқылы қосалқы Серверге қосыла аласыз. Қосалқы Сервер басты Серверден қосылым қабылдайды.

Негізгі Басқару серверін қосалқы Серверге қосу

Негізгі Сервер 13000-порт арқылы қосалқы Серверге қосылуы үшін жаңа Басқару серверін қосалқы Сервер ретінде қоса аласыз. Бұл, мысалы, егер сіз қосалқы Серверді демилитаризацияланған аймаққа орналастырсаңыз, орынды болады.

Сізге екі Басқару серверінің TCP 13291 порттары қолжетімді болып табылатын Басқару консолі орнатылған құрылғы қажет болады:

Жаңа Басқару серверін қосалқы Сервер ретінде қосу және басты Серверді оған 13000-порт арқылы қосу үшін:

1. Болашақ қосалқы Сервердің 13000-порты басты Басқару серверден қосылымдарды қабылдау үшін қолжетімді екеніне көз жеткізіңіз.

2. Басқару консолін пайдаланып, болашақ негізгі Басқару серверіне қосылыңыз.

3. Қосалқы Басқару серверін қосу жоспарланып отырған басқару тобын таңдаңыз.

4. Қажетті басқару тобының **Басқару серверлері** түйінінің жұмыс аймағында **Қосалқы Басқару серверін қосу** сілтемесі арқылы өтіңіз.

   Қосалқы Басқару серверін қосу шебері іске қосылады.

5. Шебердің бірінші қадамында (топқа қосылған Басқару серверінің мекенжайын енгізу) болашақ қосалқы Басқару серверінің желілік атауын енгізіңіз және **DMZ режимінде негізгі Басқару серверін қосалқы Басқару серверіне қосу** жалаушасын қойыңыз.

6. Болашақ қосалқы Серверге прокси-сервер арқылы қосылсаңыз, шебердің бірінші қадамында **Прокси-серверді пайдалану** жалаушасын қойып, қосылым параметрлерін енгізіңіз.

7. Содан кейін, шебердің нұсқауларын орындаңыз.

Басқару серверлерінің иерархиясы орнатылады. Қосалқы Сервер басты Серверден қосылым қабылдайды.

Басқару серверіне қосылу және Басқару серверлері арасында ауысу

Іске қосу кезінде Kaspersky Security Center бағдарламасы Басқару серверіне қосылуға әрекет жасайды. Егер желіде бірнеше Басқару сервері болса, Kaspersky Security Center бағдарламасының алдыңғы жұмыс сеансы кезінде қосылым орнатылған Сервер сұралады.

Егер Бағдарлама орнатылғаннан кейін бірінші рет іске қосылса, Kaspersky Security Center орнату кезінде көрсетілген Басқару серверіне қосылу әрекеті орындалады.

Басқару серверіне қосылғаннан кейін, сол Сервердің қалталар құрылымы консоль ағашында көрсетіледі.

Егер консоль ағашына бірнеше Басқару сервері қосылса, олардың арасында ауысуға болады.

Әрбір Басқару серверімен жұмыс істеу үшін Басқару консолі қажет. Жаңа Басқару серверіне бірінші рет қосылар алдында, онда Басқару консолінен қосылымдар қабылданатын 13291-порт және Басқару серверін Kaspersky Security Center басқа құрамдастарына байланыстыруға арналған қалған барлық порттар ашылғанына көз жеткізіңіз.

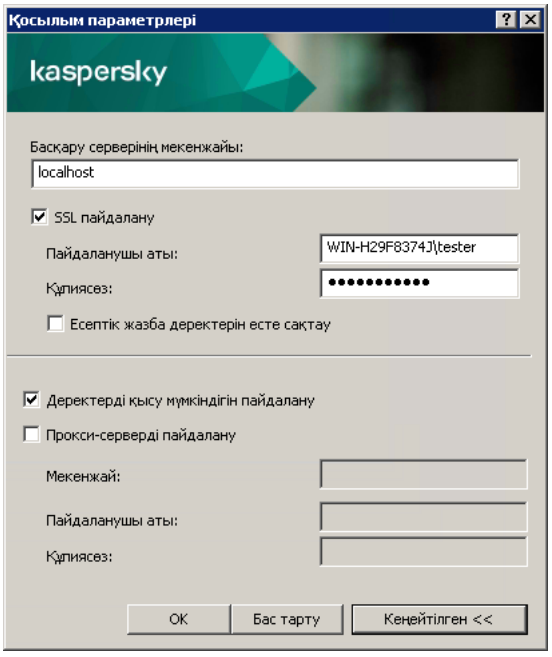
Басқа Басқару серверіне қосылу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Басқару сервері түйінінің контекстік мәзірінде **Басқару серверіне қосылу** тармағын таңдаңыз.
3. Ашылған **Қосылым параметрлері** терезесінің **Басқару серверінің мекенжайы** өрісінде, қосылғыңыз келетін Басқару серверінің атауын көрсетіңіз. Басқару сервері атауы ретінде Windows желісінде IP мекенжайын немесе құрылғы атауын көрсетуге болады. Терезенің төменгі жағындағы **Қосымша** түймесін басқан кезде Басқару серверіне қосылу параметрлерін конфигурациялауға болады (төмендегі суретті қараңыз).

   Басқару серверіне әдепкі бойынша орнатылғаннан басқа порт арқылы қосылу үшін **Басқару серверінің мекенжайы** өрісіне мәнді <Басқару серверінің атауы>:<Порт> пішімінде енгізу қажет.

   Виртуалды Басқару серверіне қосылу үшін <Басқару серверінің мекенжайы>/<виртуалды Сервер атауы> пішіміндегі **Басқару серверінің мекенжайы** өрісіне мән енгізіңіз.

Оқу құқығы жоқ пайдаланушыларға Басқару серверіне қатынасудан бас тартылады.



Басқару серверіне қосылу процесі

4. Серверлер арасында ауысуды аяқтау үшін **OK** түймесін басыңыз.

Басқару серверіне қосылғаннан кейін, консоль ағашындағы тиісті түйіннің қалталар құрылымы жаңартылады.

Басқару серверіне және оның нысандарына қатынасу құқықтары

KLAdmins және **KLOperators** пайдаланушы топтары Kaspersky Security Center орнату кезінде автоматты түрде жасалады. Бұл топтарға Басқару серверіне қосылу және оның нысандарымен жұмыс істеу құқығы беріледі.

Kaspersky Security Center бағдарламасы қандай есептік жазба арқылы орнатылып жатқанына қарамастан, **KLAdmins** және **KLOperators** топтары келесідей құрылады:

- Егер орнату доменге кіретін пайдаланушының есептік жазбасы арқылы жүргізілсе, топтар Басқару сервері кіретін доменде және Басқару серверінде құрылады.
- Егер орнату жүйенің есептік жазбасында жүргізілсе, топтар тек Басқару серверінде құрылады.

KLAdmins және **KLOperators** топтарын қарау, сондай-ақ **KLAdmins** және **KLOperators** топтары пайдаланушыларының құқықтарына қажетті өзгерістер енгізу операциялық жүйенің стандартты басқару құралдары арқылы жүзеге асырылуы мүмкін.

KLAdmins тобына барлық құқықтар, ал **KLOperators** тобына — оқу және орындау құқықтары берілген. **KLAdmins** тобына берілген құқықтар жиынтығы өзгертуге келмейді.

KLAdmins тобына кіретін пайдаланушылар *Kaspersky Security Center* әкімшілері деп, ал **KLOperators** тобының пайдаланушылары – *Kaspersky Security Center операторлары* деп аталады.

KLAdmins тобына кіретін пайдаланушылардан бөлек, Kaspersky Security Center әкімшісі құқықтары Басқару сервері орнатылған құрылғылардың жергілікті әкімшілеріне беріледі.

Жергілікті әкімшілерді Kaspersky Security Center әкімшісінің құқықтары бар пайдаланушылар тізімінен алып тастауға болады.

Kaspersky Security Center әкімшілері іске қосқан барлық операциялар Басқару серверінің есептік жазбасының құқықтарымен орындалады.

Желідегі әрбір Басқару сервері үшін осы Сервермен жұмыс істеу шеңберінде ғана құқықтарға ие өзіндік **KLAdmins** тобын құруға болады.

Егер бір доменге жататын құрылғылар әртүрлі Серверлердің басқару топтарына кіретін болса, онда домен әкімшісі барлық осы басқару топтарының ішіндегі Kaspersky Security Center әкімшісі болып табылады. Осы басқару топтарына арналған **KLAdmins** тобы біртұтас болып табылады және бірінші Басқару сервері орнатылған кезде жасалады. Kaspersky Security Center әкімшісі іске қосқан операциялар олар іске қосылған Басқару серверінің есептік жазбасының құқықтарымен орындалады.

Бағдарламаны орнатқаннан кейін Kaspersky Security Center әкімшісі келесі әрекеттерді орындай алады:

- **KLOperators** топтарына берілетін құқықтарды өзгерту;
- қауіпсіздіктің басқа топтарына және әкімшінің жұмыс орнында тіркелген жеке пайдаланушыларға Kaspersky Security Center бағдарламасының функцияларына қол жеткізу құқықтарын анықтау;
- пайдаланушылардың әр басқару тобында жұмыс істеу құқығын анықтау.

Kaspersky Security Center әкімшісі таңдалған нысанның сипаттары терезесінің **Қауіпсіздік** бөлімінде әрбір басқару тобына немесе Басқару серверінің басқа нысандарына қатынасу құқығын тағайындай алады.

Сіз Басқару серверінің жұмысындағы оқиғалар туралы жазбаларды пайдалану арқылы пайдаланушының әрекеттерін бақылай аласыз. Оқиғалар туралы жазбалар **Басқару сервері** түйінінің **Оқиғалар** қойыншасында көрсетіледі. Бұл оқиғалардың маңыздылық деңгейі **Ақпараттық оқиғалар**; оқиғалар түрлері **Аудит** сөзінен басталады.

Басқару серверіне интернет арқылы қосылу шарттары

Басқару сервері қашықта орналасса, яғни ұйымның желісінен тыс болса, клиент құрылғылар оған интернет арқылы қосылады.

Құрылғыларды интернет арқылы Басқару серверіне қосу үшін келесі шарттар орындалуы керек:

- Қашықтағы Басқару серверінде сыртқы IP мекенжайы болуы және онда 13000 кіріс порты (Желілік агенттерден қосылу үшін) ашық болуы керек. Сондай-ақ, UDP 13000 портын ашу ұсынылады (құрылғыларды өшіру туралы хабарландыруларды қабылдау үшін).
- Құрылғыларда Желілік агенттер орнатылуы керек.

- Желілік агентті құрылғыларға орнатқан кезде қашықтағы Басқару серверінің сыртқы IP мекенжайы көрсетілуі керек. Орнату үшін орнату пакеті пайдаланылса, сыртқы IP мекенжайын **Параметрлер** бөліміндегі орнату пакетінің сипаттарында қолмен көрсету қажет.

- Құрылғыға арналған қолданбалар мен тапсырмаларды басқару мақсатында қашықтағы басқару серверін пайдалану үшін құрылғының сипаттар терезесіндегі **Жалпы** бөліміндегі **Басқару серверімен байланысты үзбеу** ұяшығын таңдаңыз. Жалаушаны қойғаннан кейін, Басқару серверінің қашықтағы құрылғымен синхрондалуын күту керек. Басқару серверімен үздіксіз байланыс бір уақытта 300-ден аспайтын клиент құрылғысын қолдай алады.

Қашықтағы Басқару серверінен келетін тапсырмалардың орындалуын жеделдету үшін құрылғыда 15000 портын ашуға болады. Бұл жағдайда, тапсырманы іске қосу үшін Басқару сервері құрылғымен синхрондалуды күтпей, 15000 порты бойынша Желілік агентке арнайы пакет жібереді.

Басқару серверіне қорғалған қосылым

Клиент құрылғылары мен Басқару сервері арасында ақпарат алмасу, сондай-ақ Басқару консолін Басқару серверіне қосу TLS (Transport Layer Security) протоколының көмегімен жүзеге асырылуы мүмкін. TLS протоколы, қосылған кезде өзара әрекеттесетін тараптарды анықтауға, жіберілетін деректерді шифрлауға және оларды тасымалдау кезінде өзгерістерден қорғауға мүмкіндік береді. TLS протоколының негізінде өзара әрекеттесетін тараптардың түпнұсқалық растамасы және жалпыға ортақ кілт әдісі бойынша деректерді шифрлау жатыр.

Құрылғыны қосу кезіндегі Сервердің түпнұсқалық растамасы

Клиент құрылғысын Басқару серверіне алғаш рет қосқан кезде құрылғыдағы Желілік агент Басқару сервері сертификатының көшірмесін алады және оны жергілікті түрде сақтайды.

> Желілік агентті құрылғыға жергілікті түрде орнатқан кезде Басқару сервері сертификатын қолмен таңдауға болады.

Сертификаттың алынған көшірмесі негізінде Басқару серверінің құқықтары мен өкілеттіктері келесі қосылымдар кезінде тексеріледі.

Болашақта, құрылғыны Басқару серверіне қосқан сайын Желілік агент Басқару серверінің сертификатын сұрайды және оны жергілікті көшірмемен салыстырады. Олар бір-біріне сәйкес келмесе, Басқару серверіне құрылғыға қатынасуға рұқсат етілмейді.

Басқару консолін қосу кезінде Сервердің түпнұсқалық растамасы

Басқару серверіне алғаш рет қосылған кезде Басқару консолі Басқару серверінің сертификатын сұрайды және оның көшірмесін әкімшінің жұмыс станциясында жергілікті түрде сақтайды. Сертификаттың алынған көшірмесінің негізінде Басқару консолі осы Басқару серверіне кейіннен қосылған кезде Басқару серверін сәйкестендіру жүзеге асырылады.

Басқару серверінің сертификаты әкімшінің жұмыс станциясында сақталған сертификаттың көшірмесіне сәйкес келмесе, онда Басқару консолі берілген атаумен Басқару серверіне қосылуды растау және жаңа сертификат алу туралы сұрауды шығарады. Қосылғаннан кейін, Басқару консолі алдағыда Серверді сәйкестендіру үшін пайдаланылатын жаңа Басқару сервері сертификатының көшірмесін сақтайды.

Басқару серверіне қосылуға арналған рұқсат етілген IP мекенжайлары тізімін конфигурациялау

Әдепкі бойынша, пайдаланушылар Kaspersky Security Center Web Console веб-консолін аша алатын немесе Microsoft Management Console (MMC) негізінде Басқару консолі орнатылған кез келген құрылғыдан Kaspersky Security Center бағдарламасына кіре алады. Басқару серверін, пайдаланушылар оған тек рұқсат етілген IP мекенжайлары бар құрылғылардан қосыла алатындай етіп конфигурациялауға болады. Бұл жағдайда, егер қаскүнем Kaspersky Security Center есептік жазбасын ұрлап кетсе де, ол Kaspersky Security Center бағдарламасы кіре алмайды, өйткені қаскүнемнің құрылғысының IP мекенжайы рұқсат етілген тізімде жоқ.

IP мекенжайы пайдаланушы Kaspersky Security Center бағдарламасына кіргенде немесе Kaspersky Security Center OpenAPI арқылы басқару серверімен өзара әрекеттесетін қолданбаны іске қосқанда тексеріледі. Осы кезде пайдаланушы құрылғысы Басқару серверімен байланыс орнатуға тырысады. Құрылғының IP мекенжайы рұқсат етілгендер тізімінде болмаса, түпнұсқалық растама қатесі туындайды және KLAUD_EV_SERVERCONNECT оқиғасы Басқару серверімен қосылымның орнатылмағаны туралы хабарлайды.

Рұқсат етілген IP мекенжайлары тізіміне қойылатын талаптар

IP мекенжайлары келесі бағдарламалардың Басқару серверіне қосылу әрекеті кезінде ғана тексеріледі:

- Kaspersky Security Center Web Console Server сервері

  Егер сіз Web Console веб-консолінe бір құрылғыда кірсеңіз және Web Console сервері басқа құрылғыға орнатылған болса, онда сіз желілік экранды Web Console сервері бар құрылғыда операциялық жүйенің штаттық құралдарымен конфигурациялай аласыз. Содан кейін, егер біреу Web Console серверіне кіруге тырысса, желілік экран қаскүнемдердің жолын кесуге көмектеседі.

- Басқару консолі

- klakaut автоматтандыру нысандары арқылы Басқару серверімен өзара әрекеттесетін бағдарламалар.

- Kaspersky мақсатты шабуылдардан қорғау платформасы немесе Kaspersky Security for Virtualization сияқты OpenAPI арқылы Басқару серверімен өзара әрекеттесетін бағдарламалар.

Сондықтан, жоғарыда аталған бағдарламалар орнатылған құрылғылардың мекенжайларын көрсетіңіз.

Сіз IPv4 мекенжайлары мен IPv6 мекенжайларын орната аласыз. IP мекенжайлары ауқымдарын көрсетуге болмайды.

Рұқсат етілген IP мекенжайлары тізімін қалай жасауға болады

Егер сіз рұқсат етілген тізімді әлі орнатпаған болсаңыз, төмендегі нұсқауларды орындаңыз.

Kaspersky Security Center бағдарламасына кіру үшін рұқсат етілген IP мекенжайларының тізімін жасау үшін:

1. Басқару сервері құрылғысында әкімші құқықтары бар есептік жазбамен пәрмен жолын іске қосыңыз.

2. Ағымдағы директорияны Kaspersky Security Center орнату қалтасына өзгертіңіз (әдетте бұл <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Әкімші артықшылықтарын пайдалана отырып, келесі пәрменді теріңіз:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s`

   Жоғарыда аталған талаптарға сәйкес келетін IP мекенжайларын көрсетіңіз. Бірнеше IP мекенжайларын нүктелі үтірмен бөлу керек.

   Басқару серверіне тек бір құрылғының қосылуына рұқсат беру мысалы:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Бірнеше құрылғыға Басқару серверіне қосылуға рұқсат беру мысалы:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. Басқару сервері қызметін қайта іске қосыңыз.

Рұқсат етілген IP мекенжайларының тізімі сәтті конфигурацияланғанын Басқару серверіндегі Kaspersky Event журналынан білуге болады.

Рұқсат етілген IP мекенжайлары тізімін қалай өзгертуге болады

Сіз рұқсат етілген тізімді, оны жасау кезіндегідей өзгерте аласыз. Бұл үшін, дәл сол пәрменді орындаңыз және рұқсат етілгендердің жаңа тізімін көрсетіңіз:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s
```

Егер сіз рұқсат етілгендер тізімнен кейбір IP мекенжайларын жойғыңыз келсе, оны қайта жазыңыз. Мысалы, рұқсат етілгендер тізіміне келесі IP мекенжайлары кіреді: 192.0.2.0; 198.51.100.0; 203.0.113.0. 198.51.100.0 IP мекенжайын жойғыңыз келсе. Бұл үшін, пәрмен жолына келесі пәрменді енгізіңіз:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Басқару серверін қызметін қайта іске қосуды ұмытпаңыз.

Рұқсат етілген IP мекенжайларының конфигурацияланған тізімін қалай бастапқы мәнге келтіруге болады

Рұқсат етілген IP мекенжайларының конфигурацияланған тізімін бастапқы мәнге келтіру үшін:

1. Пәрмен жолында келесі пәрменді әкімші құқықтарымен енгізіңіз:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Басқару сервері қызметін қайта іске қосыңыз.

Осыдан кейін, IP мекенжайлары енді тексерілмейді.

13291-портты жабу үшін klscflag утилитасын пайдалану

Басқару серверінің 13291-порты Басқару консольдерінен қосылымдарды қабылдау үшін қолданылады. Әдепкі бойынша порт ашық. Егер сіз Microsoft Management Console (MMC) консолі негізіндегі Басқару консолін немесе klakaut утилитасын пайдаланғыңыз келмесе, бұл портты klscflag утилитасы көмегімен жабуға болады. Бұл утилита KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN параметрінің мәнін өзгертеді.

13291-портты жабу үшін:

1. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Пәрмен жолында келесі пәрменді орындаңыз:
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```

3. Kaspersky Security Center Басқару сервері қызметін қайта іске қосыңыз.

13291-порт жабық.

13291-порттың сәтті жабылғанын тексеру үшін:

Пәрмен жолында келесі пәрменді орындаңыз:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
ss "|ss_type = \"SS_SETTINGS\";"
```

Бұл пәрмен келесі нәтижені қайтарады:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

`false` мәні порттың жабық екенін білдіреді. Әйтпесе, `true` мәні көрсетіледі.

Басқару серверінен ажырау

Басқару серверінен ажырату үшін:

1. Консоль ағашында ажыратылатын Басқару серверіне сәйкес келетін түйінді таңдаңыз.

2. Түйіннің контекстік мәзірінде **Басқару серверінен ажырату** тармағын таңдаңыз.

Консоль ағашына Басқару серверін қосу

Консоль ағашына Басқару серверін қосу үшін:

1. Kaspersky Security Center бағдарламасының басты терезесінде, консоль ағашында **Kaspersky Security Center** түйінін таңдаңыз.

2. Түйіннің контекстік мәзірінде **Жаңа** → **Басқару сервері** тармағын таңдаңыз.

Нәтижесінде, консоль ағашында, желіде орнатылған кез келген Басқару серверіне қосылуға болатын **Басқару сервері – <Құрылғы атауы> (Қосылмаған)** атты түйін жасалатын болады.

Консоль ағашынан Басқару серверін жою

Консоль ағашынан Басқару серверін жою үшін:

1. Консоль ағашында жойылатын Басқару серверіне сәйкес келетін түйінді таңдаңыз.

2. Түйіннің контекстік мәзірінде **Жою** тармағын таңдаңыз.

Консоль шежіресіне виртуалды Басқару серверін қосу

Консоль шежіресіне виртуалды Басқару серверін қосу үшін:

1. Консоль ағашында виртуалды Басқару серверін жасау үшін қажетті Басқару сервері атауы бар түйінді таңдаңыз.

2. Басқару серверінің түйінінен **Басқару серверлері** қалтасын таңдаңыз.

3. **Басқару серверлері** қалтасының жұмыс аймағында **Виртуалды Басқару серверін қосу** сілтемесі бойынша өтіңіз.

   Виртуалды Басқару серверін жасау шебері іске қосылады.

4. **Виртуалды Басқару серверінің атауы** терезесінде жасалып жатқан виртуалды Сервердің атын көрсетіңіз.

   Виртуалды Басқару серверінің атауы 255 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

5. **Құрылғылардың виртуалды Басқару серверіне қосылу мекенжайын енгізу** терезесінде құрылғылардың қосылу мекенжайын көрсетіңіз.

   Виртуалды Басқару серверінің қосылу мекенжайы – бұл құрылғылар оған қосылатын желілік мекенжай. Қосылу мекенжайы екі бөліктен тұрады: қиғаш сызық (слеш) таңбасымен бөлінген физикалық Басқару серверінің желілік мекенжайы және виртуалды Сервердің атауы. Виртуалды Сервер атауы автоматты түрде қойылады. Көрсетілген мекенжай осы виртуалды Серверде Желілік агенттің орнату пакеттеріндегі әдепкі бойынша мекенжай ретінде пайдаланылады.

6. **Виртуалды Басқару сервері әкімшісінің есептік жазбасын жасау** терезесінде тізімнен пайдаланушының виртуалды Серверінің әкімшісін тағайындаңыз немесе **Жасау** түймесі арқылы әкімші үшін жаңа есептік жазба қосыңыз.

   Сіз бірнеше есептік жазбаны көрсете аласыз.

Нәтижесінде, Консоль ағашында **Басқару сервері – <виртуалды Сервер атауы>** атауы бар түйін жасалады.

Басқару сервері қызметінің есептік жазбасын ауыстыру. klsrvswch утилитасы

Kaspersky Security Center бағдарламасын орнату кезінде белгіленген Басқару сервері қызметінің есептік жазбасын өзгерту қажет болса, klsrvswch Басқару сервері есептік жазбасын ауыстыру утилитасын пайдалануыңызға болады.

Kaspersky Security Center орнату кезінде утилита автоматты түрде бағдарламаны орнату қалтасына көшіріледі.

Утилитаны іске қосу саны шектелмеген.

Сізге klsrvswch утилитасын Басқару серверін орнату үшін пайдаланылған әкімші құқықтары бар есептік жазба арқылы Басқару сервері құрылғысында іске қосу керек.

klsrvswch утилитасы есептік жазба түрін өзгертуге мүмкіндік береді. Мысалы, жергілікті есептік жазбаны қолдансаңыз, оны домендік есептік жазбаға немесе қызметтің басқарылатын есептік жазбасына (және керісінше) ауыстыра аласыз. klsrvswch утилитасы есептік жазба түрін қызметтің топтық басқарылатын есептік жазбасына (gMSA) өзгертуге мүмкіндік бермейді.

Windows Vista және одан кейінгі Windows нұсқалары Басқару сервері үшін LocalSystem есептік жазбасын пайдалануға мүмкіндік бермейді. Windows операциялық жүйелерінің осы нұсқаларында **LocalSystem** есептік жазбасы белсенді болмайды.

Басқару сервері қызметінің есептік жазбасын домендік есептік жазбаға өзгерту үшін:

1. klsrvswch утилитасын Kaspersky Security Center орнату қалтасынан іске қосыңыз. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Нәтижесінде, Басқару серверінің қызметтік есептік жазбасын өзгерту шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

2. **Басқару сервері қызметінің есептік жазбасы** терезесінде **LocalSystem есептік жазбасы** тармағын таңдаңыз.

Шебер жұмысының нәтижесінде, Басқару сервері есептік жазбасы өзгертіледі. Басқару сервер қызметі *LocalSystem* есептік жазбасымен іске қосылады және оның есептік деректерін пайдаланады.

Kaspersky Security Center дұрыс жұмыс істеуі үшін, Басқару сервер қызметін іске қосуға арналған есептік жазба Басқару серверінің ақпараттық дерекқорын орналастыруға арналған ресурс әкімшісінің құқықтарына ие болуы қажет.

Басқару сервері қызметінің есептік жазбасын пайдаланушы есептік жазбасына немесе қызметтің басқарылатын есептік жазбасына өзгерту үшін:

1. klsrvswch утилитасын Kaspersky Security Center орнату қалтасынан іске қосыңыз. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Нәтижесінде, Басқару серверінің қызметтік есептік жазбасын өзгерту шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

2. **Басқару сервері қызметінің есептік жазбасы** терезесінде **Пайдаланушы есептік жазбасы** тармағын таңдаңыз.

3. **Қазір табу** түймесін басыңыз.

   Пайдаланушыларды таңдау терезесі ашылады.

4. **Пайдаланушыларды таңдау** терезесінде **Нысан түрлері** түймесін басыңыз.

5. Нысан түрлері тізімінде **Пайдаланушылар** (пайдаланушы есептік жазбасын қолданғыңыз келсе) немесе **Қызметтерге арналған есептік жазба** (қызметтің басқарылатын есептік жазбасын қолданғыңыз келсе) тармағын таңдаңыз да, **OK** түймесін басыңыз.

6. Нысанның атына арналған өрісте есептік жазба атауын немесе атауының бөлігін енгізіңіз және **Атауларды тексеру** түймесін басыңыз.

7. Тиісті атаулар тізімінде қажетті атауды таңдап, **OK** түймесін басыңыз.

8. **Қызметтердің есептік жазбалары** тармағын таңдасаңыз, **Есептік жазбаның құпиясөзі** терезесінде **Құпиясөз** бен **Құпиясөзді растау** өрістерін бос қалдырыңыз. **Пайдаланушылар** тармағын таңдаған болсаңыз, пайдаланушыға арналған құпиясөзді енгізіп, оны растаңыз.

Басқару сервері қызметінің есептік жазбасы сіз таңдаған есептік жазбамен іске қосылады.

Microsoft SQL серверін Windows құралдарымен пайдаланушы есептік жазбасының түпнұсқалық растамасы режимінде пайдаланған кезде дерекқорға қатынасуды қамтамасыз ету қажет. Пайдаланушы есептік жазбасы Kaspersky Security Center дерекқорының иесі болуы тиіс. Әдепкі бойынша, dbo схемасын қолдану керек.

ДҚБЖ есептік деректерін өзгерту

Кейде ДҚБЖ есептік жазба деректерін өзгерту қажет болуы мүмкін (мысалы, қауіпсіздік мақсатында есептік жазба деректерінің ротациясын орындау үшін).

klsrvswch.exe утилитасын пайдаланып Windows ортасында ДҚБЖ есептік деректерін өзгерту үшін:

1. Kaspersky Security Center орнату қалтасында орналасқан klsrvswch утилитасын іске қосыңыз. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Сізге klsrvswch утилитасын Басқару серверін орнату үшін пайдаланылған әкімші құқықтары бар есептік жазба арқылы Басқару сервері құрылғысында іске қосу керек.

2. Шебердің **Келесі** түймесін **ДҚБЖ қатынасу есептік жазба деректемелерін өзгерту** қадамына дейін жетпейінше баса беріңіз.

3. Шебердің **ДҚБЖ қатынасу есептік жазба деректемелерін өзгерту** қадамында келесі әрекеттерді орындаңыз:

   Windows аутентификациясы пайдаланылса, шебердің **ДҚБЖ қатынасу есептік жазба деректемелерін өзгерту** қадамы өткізіледі.

   - **Жаңа есептік жазба деректемелерін қолданыңыз** параметрін таңдаңыз.
   - **Есептік жазба** өрісінде есептік жазбаның жаңа атауын көрсетіңіз.
   - **Құпиясөз** өрісінде есептік жазба үшін жаңа құпиясөзді көрсетіңіз.
   - **Құпиясөзді растау** өрісінде жаңа құпиясөзді растаңыз.

   ДҚБЖ-да бұрыннан бар есептік жазбаның есептік деректерін көрсетуіңіз керек.

4. **Келесі** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін, ДҚБЖ есептік деректері өзгертіледі.

klsrvswch утилитасын тек SQL аутентификациясына арналған есептік жазба құпиясөзін өзгерту үшін пайдалануға болады. Авторизация әдісін өзгертуге қолдау көрсетілмейді. Авторизация әдісін өзгерту үшін басқару серверін қайта орнатып, қажетті параметрлерді көрсетіңіз.

Басқару серверінің ортақ қатынасы бар қалтасын өзгерту

Басқару серверінің ортақ қатынасы бар қалтасы Басқару серверін орнату кезінде көрсетіледі. Ортақ қатынасы бар қалтаның орнын Басқару серверінің сипаттарында өзгертуге болады.

Ортақ қатынасы бар қалтаны өзгерту үшін:

1. **Барлығы** ішкі тобына толық басқару құқықтарын беру үшін ортақ желілік қалтаны жасаңыз және ортақ қалта мен қалта құрылымында рұқсаттарды теңшеңіз.

2. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

3. Басқару серверінің сипаттар терезесінде **Бөлімдер** панелінде **Кеңейтілген** бөліміне өтіңіз және **Басқару серверінің ортақ қатынас бар қалтасы** таңдаңыз.

4. **Басқару серверінің ортақ қатынас бар қалтасы** бөлімінде **Өзгерту** түймесін басыңыз.

5. Ортақ қатынасы бар қалта ретінде қолданғыңыз келетін қалтаны таңдаңыз.

6. Басқару сервері сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

7. Ортақ қатынасы бар қалта ретінде таңдалған қалта үшін **Барлығы** ішкі тобына оқу рұқсаттарын тағайындау.

Басқару сервері түйіндерінің мәселелерін шешу

Басқару консолінің сол жақ тақтасындағы ағашта Басқару серверіне сәйкес келетін түйіндер бар. Сіз консоль ағашын Басқару серверлерінің қажетті санына қоса аласыз.

Microsoft Management Console (MMC) Басқару консолі консоль ағашындағы Басқару сервері түйіндерінің тізімін .msc файлының көлеңкелі көшірмесіне сақтайды. Бұл файлдың көлеңкелі көшірмесі, Басқару консолі орнатылған құрылғыдағы %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ қалтасында сақталады. Басқару серверінің әрбір түйіні үшін файлда келесі ақпарат қамтылған:

- Басқару сервері мекенжайы
- Порт нөмірі
- TLS қолданылады ма

  Бұл параметр, Басқару консолін Басқару серверіне қосу үшін қолданылатын порт нөміріне тәуелді.
- Пайдаланушы аты
- Басқару сервері сертификаты

Ақаулықтарды жою

Басқару консолін Басқару серверіне қосу кезінде жергілікті сақталған сертификат Басқару сервері сертификатымен салыстырылады. Егер сертификаттар сәйкес бір-біріне келмесе, Басқару консолінде қате пайда болады. Сертификаттардың бір-біріне сәйкес келмеуі, мысалы, Басқару сервер сертификатын ауыстыру кезінде орын алуы мүмкін. Бұл жағдайда, консольде Басқару сервері түйінін қайта құру қажет.

Басқару сервері түйінін қайта құру үшін:

1. Kaspersky Security Center Басқару консолі терезесін жабыңыз.
2. %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ қалтасынан Kaspersky Security Center 15.1 файлын жойыңыз.
3. Kaspersky Security Center Басқару консолін іске қосыңыз.

   Басқару серверіне қосылу және оның бар сертификатын қабылдау туралы ұсыныс көрсетіледі.
4. Келесі әрекеттердің бірін орындаңыз:

   - **Иә** түймесін басу арқылы, қолданыстағы сертификатты қабылдаңыз.
   - Өз сертификатыңызды көрсету үшін, **Жоқ** түймесін басыңыз және Басқару серверінің түпнұсқалық растамасы үшін қолданылатын сертификат файлына өтіңіз.

Сертификатпен байланысты мәселе шешілді. Басқару серверіне қосылу үшін Басқару консолін пайдалануға болады.

Басқару сервері параметрлерін қарау және өзгерту

Басқару сервері параметрлерін Басқару сервері сипаттары терезесінде конфигурациялауға болады.

Сипаттар терезесін ашу үшін: Басқару сервері,

консоль ағашындағы Басқару сервері түйінінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

Басқару серверінің жалпы параметрлерін көрсету

Сіз Басқару сервері сипаттары терезесінің **Жалпы**, **Басқару серверіне қосылу параметрлері**, **Оқиғалар қоймасы** және **Қауіпсіздік** бөлімдерінде Басқару серверінің жалпы параметрлерін конфигурациялай аласыз.

Басқару консолі интерфейсінде, оның дисплейі өшірулі болса, Басқару сервері сипаттары терезесінде **Қауіпсіздік** бөлімі көрсетілмейді.

*Басқару консолінде **Қауіпсіздік** бөлімінің көрсетілуін қосу үшін:*

1. Консоль ағашында қажетті Басқару серверін таңдаңыз.
2. Бағдарламаның басты терезесінің **Көру** мәзірінде **Интерфейсті конфигурациялау** тармағын таңдаңыз.
3. Ашылған **Интерфейсті конфигурациялау** терезесінде **Қауіпсіздік параметрлері бар тарауларды көрсету** жалаушасын қойып, **OK** түймесін басыңыз.
4. Бағдарлама хабары бар терезеде **OK** түймесін басыңыз.

Қауіпсіздік бөлімі Басқару сервері сипаттары терезесінде көрсетіледі.

Басқару консолі интерфейсінің параметрлері

Басқару консолі интерфейсінің параметрлерін келесі функцияларға қатысты пайдаланушы интерфейсінің басқару элементтерін көрсету немесе жасыру үшін конфигурациялауға болады:

- Осалдықтар мен патчтарды басқару
- Деректерді шифрлау және қорғау
- Соңғы нүктелерді басқару параметрлері
- Ұялы құрылғыларды басқару
- Қосалқы Басқару серверлері
- Қауіпсіздік параметрлері бар бөлімдер

Басқару консолі интерфейсінің параметрлерін конфигурациялау үшін:

1. Консоль ағашында қажетті Басқару серверін таңдаңыз.
2. Бағдарламаның басты терезесінің **Көру** мәзірінде **Интерфейсті конфигурациялау** тармағын таңдаңыз.

3. Ашылған **Интерфейсті конфигурациялау** терезесінде, көрсетілуі тиісті функционалдылықтың жанына жалаушаны қойып, **OK** түймесін басыңыз.

4. Бағдарлама хабары бар терезеде **OK** түймесін басыңыз.

Таңдалған функционалдылық Басқару консолі интерфейсінде көрсетіледі.

Басқару серверінде оқиғаларды өңдеу және сақтау

Қолданба мен басқарылатын құрылғылар жұмысы кезінде орын алатын оқиғалар туралы ақпарат басқару серверінің дерекқорына сақталады. Әрбір оқиға белгілі бір түрге және маңыздылық деңгейіне қатысты болып келеді (*Критикалық оқиға*, *Функционалдық ақау*, *Ескерту*, *Ақпараттық хабарлар*). Оқиға болған жағдайларға байланысты, бағдарлама бір типті оқиғаларға әртүрлі маңыздылық деңгейлерін бере алады.

Оқиғалардың түрлері мен маңыздылық деңгейлерін Басқару сервері сипаттары терезесінің **Оқиғаны конфигурациялау** бөлімінен көруге болады. **Оқиғаны конфигурациялау** бөлімінде сіз әрбір оқиғаны Басқару сервері тарапынан өңдеу параметрлерін де конфигурациялай аласыз:

- құрылғы мен Басқару серверіндегі операциялық жүйе оқиғалары журналдарында және Басқару серверінде оқиғаларды тіркеу;
- әкімшіні оқиға туралы хабарландыру тәсілі (мысалы, SMS, электрондық пошта хабарламасы).

Басқару сервері сипаттары терезесінің **Оқиғалар қоймасы** бөлімінде Басқару серверінің дерекқорында оқиғаларды сақтау параметрлерін конфигурациялауға болады: оқиғалар туралы жазбалар санын және жазбаларды сақтау уақытын шектеу. Оқиғалардың ең көп санын көрсеткенде, бағдарламалар оқиғалардың көрсетілген санын сақтау үшін диск кеңістігінің долбарлы өлшемін есептейді. Сіз бұл есептеуді дерекқордың толып кетуіне жол бермеу үшін бос диск кеңістігінің жеткілікті ме екенін бағалау үшін пайдалана аласыз. Әдепкі бойынша, Басқару сервері дерекқорының сыйымдылығы 400 000 оқиғаны құрайды. Дерекқордың ұсынылған ең жоғары сыйымдылығы 45 000 000 оқиғаны құрайды.

Бағдарлама дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, бағдарлама оқиғалардың көрсетілген ең көп саны ғана қалуы үшін ең ескі оқиғаларды жояды.

Басқару сервері ескі оқиғаларды жойған кезде, ол жаңа оқиғаларды дерекқорға сақтай алмайды. Осы кезең ішінде қабылданбаған оқиғалар туралы ақпарат Kaspersky Event журналына жазылады. Жаңа оқиғалар кезекке қойылады, содан соң жою операциясы аяқталғаннан кейін, дерекқорда сақталады.

Тапсырманы орындау барысына қатысты оқиғаларды сақтау немесе тек тапсырманы орындау нәтижелерін сақтау үшін кез келген тапсырманың параметрлерін өзгертуге болады. Осылайша, сіз дерекқордағы оқиғалардың санын азайтасыз, дерекқордағы оқиғалар кестесін талдаумен байланысты сценарийлердің жұмыс жылдамдығын арттырасыз және критикалық оқиғаларды оқиғалардың көп санымен ығыстыру қаупін азайтасыз.

Басқару серверіне Қосылымдар журналдарын қарау

Басқару серверінің жұмысы барысында, оған қосылымдар мен қосылым әрекеттері тарихын журнал файлына сақтауға болады. Файлдағы ақпарат желі инфрақұрылымы ішіндегі қосылымдарды ғана емес, Басқару серверіне рұқсатсыз қатынасу әрекеттерін де қадағалауға мүмкіндік береді.

Басқару серверіне қосылым оқиғаларын тіркеуді конфигурациялау үшін:

1. Консоль ағашынан, қосылым оқиғаларын тіркеуді қосу қажет Басқару серверін таңдаңыз.

2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. **Басқару серверіне қосылу параметрлері** бөлімінде ашылған сипаттар терезесінде салынған **Қосылу порттары** бөлімін таңдаңыз.

4. **Басқару серверінің байланыс оқиғаларын журналға тіркеу** параметрін қосыңыз.

5. Басқару сервері сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

Басқару серверіне кіріс қосылымдарының барлық кейінгі оқиғалары, түпнұсқалық растама нәтижелері және SSL қателері %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog файлына жазылатын болады.

Вирустық індеттердің туындауын бақылау

Kaspersky Security Center бағдарламасысізге вирустық індеттер қаупінің туындауына уақтылы ден қоюға мүмкіндік береді. Вирустық індет қаупін бағалау құрылғылардағы вирустық белсенділікті бақылау арқылы жүзеге асырылады.

Сіз вирустық індет қаупін бағалау ережелерін және егер ол орын алса, Басқару сервері сипаттары терезесінің **Вирустық шабуыл** бөлімінде конфигурациялай аласыз.

Вирустың тарауы оқиғасы туралы хабарландыру тәртібі Басқару сервері сипаттары терезесінің **Оқиғаларды конфигурациялау** бөлімінде, *Вирустың тарауы* оқиғасы сипаттары терезесінде белгіленуі мүмкін.

Вирустың тарауы оқиғасы, қауіпсіздік бағдарламаларының жұмысында *Зиянды нысан анықталды* оқиғалары анықталған кезде туындайды. Сол себепті, вирустық індетті тану үшін *Зиянды нысан анықталды* оқиғалары туралы ақпаратты Басқару серверінде сақтау керек.

Зиянды нысан анықталды оқиғасы туралы ақпаратты сақтау параметрлері қауіпсіздік бағдарламалары саясаттарында белгіленеді.

Зиянды нысан анықталды оқиғаларын есептеу кезінде, тек негізгі Басқару серверінен алынған ақпарат қана ескеріледі. Қосалқы Басқару серверлерінен алынған ақпарат есепке алынбайды. Әрбір қосалқы Сервері үшін *Вирустың тарауы* оқиғасының параметрлерін жеке-жеке конфигурациялау керек.

Трафикті шектеу

Желідегі трафикті азайту үшін бөлек IP ауқымдарынан және IP аралықтарынан Басқару серверіне деректерді беру жылдамдығын шектеу мүмкіндігі қарастырылған.

Сіз Басқару сервері сипаттары терезесінің **Трафик** бөлімінде трафикті шектеу ережелерін жасап, конфигурациялай аласыз.

Трафикті шектеу ережелерін жасау үшін:

1. Консоль ағашында трафикті шектеу ережелерін жасау үшін қажетті Басқару сервері атауы бар түйінді таңдаңыз.

2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесінде **Трафик** бөлімін таңдаңыз.

4. **Қосу** түймесін басыңыз.

5. **Жаңа ереже** бөлімінде келесі параметрлерді көрсетіңіз:

   Трафикті шектеуге арналған IP ауқымы блогында, беру жылдамдығы шектелген ішкі желіні немесе ауқымды белгілеу тәсілін таңдап, таңдалған тәсіл үшін параметрлердің мәндерін көрсетуге болады. Келесі тәсілдердің бірін таңдаңыз:

   - **Мекенжайлар мен желі маскасы арқылы ауқымды көрсету**

     Трафик ішкі желі параметрлері бойынша шектеледі. Трафик шектелетін аралықты анықтау үшін ішкі желі мекенжайын және ішкі желі бүркенішін енгізу өрістерінде көрсетіңіз.

     Шолу түймесін басып, глобалды қосалқы желілердің тізімінен ішкі желіні қосыңыз.

   - **Бастапқы және соңғы мекенжайлар арқылы ауқымды көрсету**

     Трафик IP мекенжайы аралығы бойынша шектеледі. **Бастапқы IP мекенжайы** және **Соңғы IP мекенжайы** енгізу өрістерінде IP мекенжайлары аралығын көрсетіңіз.

     Әдепкі бойынша, осы нұсқа таңдалады.

   Трафикті шектеу блогында деректерді беру жылдамдығын шектеудің келесі параметрлерін конфигурациялауға болады:

   - **Уақыт аралығы**

     Трафиктің шектеуі қолданылатын уақыт аралығы. Уақыт аралығының шекараларын енгізу өрістерінде көрсетуге болады.

   - **Шектеу (КБ/сек)**

     Басқару серверінің кіріс және шығыс деректерін берудің жиынтық жылдамдығының шекті мәні. Шектеу **Кезең** өрісінде көрсетілген уақыт аралығында ғана әрекет етеді.

   - **Қалған уақытта трафикті шектеу (КБ/сек)**

     Трафик **Кезең** өрісінде көрсетілген аралық ішінде ғана емес, қалған уақыт бойы да шектеледі.

     Әдепкі бойынша, жалауша алынып тасталған. Өріс мәні **Шектеу (КБ/сек)** өрісінің мәніне сай келмеуі мүмкін.

Ең алдымен, трафикті шектеу ережелері файлдарды тасымалдауға әсер етеді. Бұл ережелер Басқару сервері мен Желілік агент арасында немесе негізгі Басқару сервері мен қосалқы Басқару сервері арасында синхрондау кезінде пайда болатын трафикке қолданылмайды.

Веб-сервер параметрлерін конфигурациялау

Веб-сервер жеке орнату пакеттерін, iOS MDM профильдерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды жариялау үшін қолданылады.

Сіз Веб-Серверді Басқару серверіне қосу параметрлерін конфигурациялай аласыз және Веб-сервер сертификатын Басқару сервері сипаттары терезесінің **Веб-сервер** бөлімінен белгілей аласыз.

Ішкі пайдаланушылармен жұмыс істеу

Ішкі пайдаланушы есептік жазбалары виртуалды Басқару серверлерімен жұмыс істеу үшін пайдаланылады. Kaspersky Security Center бағдарламасында ішкі пайдаланушылар шынайы пайдаланушы құқықтарына ие.

Ішкі пайдаланушы есептік жазбалары тек Kaspersky Security Center ішінде жасалады және пайдаланылады. Ішкі пайдаланушылар туралы мәліметтер операциялық жүйеге берілмейді. Ішкі пайдаланушылардың аутентификациясын Kaspersky Security Center жүзеге асырады.

Сіз ішкі пайдаланушы есептік жазбаларының параметрлерін консоль ағашының **Пайдаланушылардың есептік жазбалары** қалтасында конфигурациялай аласыз.

Басқару сервері параметрлерін сақтық көшірмелеу және қалпына келтіру

Басқару серверінің параметрлерін және ол қолданатын дерекқорды сақтық көшірмелеу үшін сақтық көшірмелеу тапсырмасы және klbackup утилитасы қарастырылған. Сақтық көшірме Басқару серверінің барлық негізгі параметрлері мен нысандарын қамтиды: Басқару серверінің сертификаттары, басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері, лицензияларға арналған кілттер, барлық мазмұны, тапсырмалары, саясаттары және тағы басқасы бар басқару топтарының құрылымы. Сақтық көшірмеге ие болып, Басқару серверінің жұмысын аз уақытта - ондаған минуттан екі сағатқа дейін қалпына келтіруге болады.

Сақтық көшірме болмаса, ақау сертификаттардың және Басқару серверінің барлық параметрлерінің қайтарымсыз жоғалуына әкелуі мүмкін. Бұл Kaspersky Security Center қайтадан конфигурациялау, сондай-ақ ұйымның желісінде Желілік агентті бастапқы орналастыруды қайтадан орындау қажеттілігіне әкеледі. Сонымен қатар, басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері де жоғалады, бұл Kaspersky Endpoint Security-мен құрылғыларда шифрланған деректердің қайтарымсыз жоғалу қаупін тудырады. Сондықтан сақтық көшірудің штаттық тапсырмасы көмегімен Басқару серверінің сақтық көшірмелерін үнемі жасаудан бас тарту керек.

Жылдам іске қосу шебері басқару сервері параметрлерінің сақтық көшірме тапсырмасын жасайды және оны күнде 04:00-де іске қосылатындай орнатады. Сақтық көшірмелер әдепкісінше %ALLUSERSPROFILE%\Application Data\KasperskySC қалтасында сақталады.

Егер ДҚБЖ ретінде басқа құрылғыға орнатылған Microsoft SQL Server данасы қолданылса, сақтық көшірмелеу тапсырмасын өзгерту керек: жасалған сақтық көшірмелерді сақтау қалтасы ретінде Басқару серверінің қызметіне де, SQL Server қызметіне де жазу үшін қолжетімді UNC-жолын көрсету керек. Бұл талап Microsoft SQL Server ДҚБЖ үшін сақтық көшірмелеудің нәтижесі болып табылады.

Егер ДҚБЖ ретінде Microsoft SQL Server жергілікті данасы пайдаланылса, оларды бір уақытта Басқару серверімен зақымданудан қорғау үшін бөлек тасығышта сақтық көшірмелерді сақтау ұсынылады.

Сақтық көшірме маңызды деректерді қамтиды, сондықтан сақтық көшірмелеу тапсырмасында және klbackup утилитасында сақтық көшірмелерді құпиясөзбен қорғау қарастырылған. Әдепкі бойынша сақтық көшірмелеу тапсырмасы бос құпиясөзбен жасалады. Сақтық көшірмелеу сипаттарында құпиясөзді міндетті түрде белгілеу керек. Бұл талапты сақтамау Басқару серверінің сертификаттарының кілттері, лицензияларға арналған кілттер және басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері шифрланбаған болатынына әкеледі.

Үнемі сақтық көшірмелеумен қатар, барлық маңызды өзгерістердің алдында, соның ішінде Басқару серверін жаңа нұсқаға дейін жаңартудың алдында және Басқару серверінің патчтарын орнатудың алдында сақтық көшірмені жасау керек.

Егер ДҚБЖ ретінде Microsoft SQL Server қолдансаңыз, сіз сақтық көшірмелердің өлшемін барынша азайта аласыз. Бұл үшін SQL Server параметрлерінде **Сақтық көшірмелерді сығу (Compress backup)** жалаушасын орнатыңыз.

Сақтық көшірмеден қалпына келтіру klbackup утилитасы көмегімен сақтық көшірме жасалған нұсқадағы (немесе барынша жаңа) Басқару серверінің жаңа ғана орнатылған және жұмысқа қабілетті данасында орындалады.

Қалпына келтіру орындалатын Басқару серверінің инсталляциясы дәл сол немесе барынша жаңа нұсқадағы сондай түрдегі (мысалы, SQL Server немесе MariaDB) ДҚБЖ пайдалануы тиіс. Басқару серверінің нұсқасы сондай (ұқсас немесе барынша жаңа патчпен) немесе барынша жаңа болуы мүмкін.

Осы бөлімде параметрлерді және Басқару серверінің нысандарын қалпына келтірудің типтік сценарийлері сипатталған.

Сақтық көшірмелеу уақытын азайту үшін файлдық жүйенің суретін пайдалану

Kaspersky Security Center 15.1 бағдарламасында, деректерді сақтық көшірмелеу кезінде Басқару серверінің бос тұру уақыты одан да ерте нұсқаларымен салыстырғанда азайтылған. Бұдан бөлек, тапсырманың параметрлеріне **Деректердің резервтік қоймасы үшін файлдық жүйенің суретін пайдалану** функциясы қосылған. Бұл функция бос тұру уақытынша қосымша түрде азайтуға мүмкіндік береді, себебі klbackup утилитасы сақтық көшірмелеу кезінде дискінің көлеңкелі көшірмесін жасайды (бұған бірнеше секунд кетеді) және бір мезгілде дерекқорды көшірмелейді (бұған кемінде бірнеше минут кетеді). Дискінің көлеңкелі көшірмесін және дерекқордың көшірмесін жасап, klbackup утилитасы Басқару серверін қосылуға қолжетімді етеді.

Сіз файлдық жүйе суретін жасау функциясын келесі екі шарт сақталғанда ғана қолдана аласыз:

- Басқару серверіның ортақ қатынасы бар қалтасы және %ALLUSERSPROFILE%\KasperskyLab қалтасы бір жергілікті дискіде орналасқан және Басқару серверіне қатысты тұрғыда жергілікті болып келеді.
- %ALLUSERSPROFILE%\KasperskyLab қалтасының ішінде қолмен жасалған таңбалық сілтемелер жоқ.

Осы шарттардың кемінде біреуі орындалмаса, функцияны қолданбаңыз. Файлдық жүйе суретін жасау әрекетіне жауап ретінде, бағдарлама қате туралы хабар жібереді.

Функцияны қолдану үшін, %ALLUSERSPROFILE% қалтасы орналасқан логикалық дискі суреттерін жасау құқықтары бар есептік жазба болуы керек. Басқару сервері қызметінің есептік жазбасының мұндай құқықтары жоқ.

Сақтық көшірмелеу уақытын азайту мақсатымен файлдық жүйе суретін жасау функциясын пайдалану үшін:

1. **Тапсырмалар** бөлімінде сақтық көшірмелеу тапсырмасын таңдаңыз.
2. Мәнмәтіндік мәзірден **Сипаттар** тармағын таңдаңыз.
3. Пайда болған тапсырма сипаттары терезесінде **Параметрлер** бөлімін таңдаңыз.
4. **Деректердің резервтік қоймасы үшін файлдық жүйенің суретін пайдалану** жалаушасын қойыңыз.
5. **Пайдаланушы аты** мен **Құпиясөз** өрістерінде, %ALLUSERSPROFILE% қалтасы орналасқан логикалық диск суреттерін жасау құқығы бар есептік жазбаның атауы мен құпиясөзін енгізіңіз.
6. **Қолдану** түймесін басыңыз.

Сақтық көшірмелеу тапсырмасын келесі жолы іске қосқан кезде, klbackup утилитасы файлдық жүйенің суреттерін жасайды, ал тапсырманы орындау кезінде Басқару серверінің бос тұру уақыты қысқарады.

Басқару сервері бар құрылғы істен шықты

Егер ақау нәтижесінде Басқару сервері бар құрылғы істен шықса, келесі әрекеттерді орындау ұсынылады:

- Жаңа Серверге сол мекенжайды тағайындау: NetBIOS-атауы, FQDN-атауы, статикалық IP - Желілік агентті орналастырған кезде қайсысы белгіленгеніне байланысты.
- Сол немесе барынша жаңа нұсқада, сондай түрдегі ДҚБЖ қолдана отырып Басқару серверін орнату. Сол немесе барынша жаңа патчы бар Сервердің нұсқасын немесе барынша жаңа нұсқаны орнатуға болады. Орнатқан соң шебердің көмегімен бастапқы конфигурациялауды орындамаған жөн.
- **Іске қосу** мәзірінен klbackup сақтық көшірмелеу утилитасын іске қосыңыз және қалпына келтіруді орындаңыз.

Басқару серверінің параметрлері немесе дерекқор зақымдалған

Егер Басқару сервері параметрлердің немесе дерекқордың зақымдалуы нәтижесінде жұмысқа қабілетсіз болса (мысалы, қуат ақаулығы себебінен), қалпына келтірудің келесі сценарийін қолдану ұсынылады:

1. Зақымданған құрылғыда файлдық жүйені тексеруді орындау.
2. Басқару серверінің жұмысқа қабілетсіз нұсқасын деинсталляциялау.
3. Сол түрдегі, сол немесе барынша жаңа нұсқадағы ДҚБЖ қолдана отырып Басқару серверін қайтадан орнату. Сол немесе барынша жаңа патчы бар Сервердің нұсқасын немесе барынша жаңа нұсқаны орнатуға болады. Орнатқан соң шебердің көмегімен бастапқы конфигурациялауды орындамаған жөн.
4. **Іске қосу** мәзірінен klbackup сақтық көшірмелеу утилитасын іске қосыңыз және қалпына келтіруді орындаңыз.

Басқару серверін klbackup штаттық утилитасынан басқа кез келген тәсілмен қалпына келтіруге болмайды.

Серверді бөтен бағдарламалық жасақтаманың көмегімен қалпына келтірудің барлық жағдайларында Kaspersky Security Center таратылған бағдарламасының түйіндерінде деректердің синхронизациясы бұзылады.

Басқару сервері деректерін сақтық көшірмелеу және қалпына келтіру

Деректердің сақтық көшірмесі Басқару серверін бір құрылғыдан екіншісіне ақпаратты жоғалтпай тасымалдауға мүмкіндік береді. Сақтық көшірме жасау арқылы басқару сервері дерекқорын басқа құрылғыға жылжытқанда немесе Kaspersky Security Center бағдарламасының жаңа нұсқасына жаңартқанда деректерді қалпына келтіре аласыз. Сонымен қатар Басқару сервері деректерін Kaspersky Security Center Linux басқаруындағы Kaspersky Security Center Windows жүйесінен жылжыту үшін деректердің сақтық көшірмесін пайдалануға болады (деректерді Kaspersky Security Center Linux жүйесінен Kaspersky Security Center Windows жүйесіне жылжытуға қолдау көрсетілмейді).

Орнатылған басқару плагиндерінің сақтық көшірмелері сақталмайтынын ескеріңіз. Сақтық көшірмеден Басқару сервері деректерін қалпына келтіргеннен кейін, басқарылатын бағдарлама плагиндерін жүктеп, қайта орнату қажет.

Басқару сервер деректерінің сақтық көшірмесін жасамас бұрын, басқару тобына виртуалды Басқару серверінің қосылғанын тексеріңіз. Сақтық көшірме жасау алдында виртуалды Басқару сервер қосылса, осы виртуалды серверге әкімші тағайындалғанын тексеріңіз. Сақтық көшірмеден кейін виртуалды Басқару серверге әкімші құқықтарын бере алмайсыз. Әкімшінің тіркелгі деректері жоғалса, виртуалды әкімші серверіне жаңа әкімші тағайындай алмайтыныңызды ескеріңіз.

Kaspersky Security Center ақауларға төзімді кластерінің сақтық көшірмесін жасау немесе қалпына келтіру үшін бүкіл кластерді техникалық қызмет көрсету үшін тоқтатып, сақтық көшірме жасау немесе қалпына келтіру аяқталғаннан кейін оны қайта іске қосу керек.

Басқару сервері деректерінің сақтық көшірмесін келесі тәсілдердің бірімен жасауға болады:

- Басқару консолі арқылы деректерді сақтық көшірмелеу тапсырмасын жасау және іске қосу.
- Басқару сервері орнатылған құрылғыда klbackup утилитасын іске қосу. Утилита Kaspersky Security Center жеткізу жиынтығының құрамына кіреді. Басқару серверін орнатқаннан кейін, утилита бағдарламаны орнату кезінде көрсетілген мақсатты қалтаның түбірінде болады.

Басқару сервері деректерінің сақтық көшірмесінде келесі деректер сақталады:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері).
- Басқару топтары құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат.
- Қашықтан орнатуға арналған бағдарлама дистрибутивтері қоймасы.
- Басқару сервері сертификаты.

- *Жаңартулар* қалтасының мазмұны.

  Әдепкісінше қалта жолы — C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Басқару сервері деректерін тек klbackup утилитасының көмегімен қалпына келтіруге болады. Жаңа ғана орнатылған және сақтық көшірме жасалған нұсқамен бірдей (немесе одан кейінгі) басқару серверінің жұмыс істейтін данасында ғана қалпына келтіруге болады.

Басқару сервері деректерін сақтық көшірмелеу тапсырмасы

Басқару сервері деректерін сақтық көшірмелеу тапсырмасын жасау

Сақтық көшірмелеу тапсырмасы басқару серверінің тапсырмасы болып табылады; ол бастапқы орнату шеберінің көмегімен жасалады. Бағдарламаны жылдам іске қосу шебері жасаған сақтық көшірмелеу тапсырмасы жойылса, оны қолмен жасауға болады.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.

2. Жасау процесін келесі тәсілдердің бірімен іске қосыңыз:

   - Консоль тармағындағы **Тапсырмалар** қалтасының контекстік мәзіріндегі Тапсырма → **Тапсырмалар** тармағын таңдау арқылы.

   - Жұмыс аймағыдағы **Тапсырма жасау** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз. Шебердің **Тапсырма түрін таңдау** терезесінде **Басқару сервері деректерінің резервтік қоймасы** тапсырма түрін таңдаңыз.

Басқару сервері деректерінің резервтік қоймасы тапсырмасын тек бір үлгіде ғана жасауға болады. Басқару сервері деректерін сақтық көшірмелеу тапсырмасы Басқару сервері үшін жасалған болса, онда ол сақтық көшірмелеу тапсырмасын жасау шеберінің тапсырма түрін таңдау терезесінде көрсетілмейді.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын конфигурациялау

Сақтық көшірмелеу тапсырмасын жасағаннан кейін, тапсырма параметрлерін реттеуге болады.

Басқару сервер деректерінің сақтық көшірмесін жасау тапсырмасының параметрлерін конфигурациялау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Басқару сервері деректерінің резервтік қоймасы** тапсырмасының мәтінмәндік мәзірінде **Сипаттар** тармағын таңдаңыз.

Басқару сервері деректерінің сақтық көшірмесін жасау тапсырмасына арналған сипаттар терезесі ашылады. Келесі сипаттар қолжетімді:

- **Жалпы**

  Жалпы бөлімінде тапсырма атауын көрсетуге, тапсырма жасалған күнді, соңғы пәрменнің күнін, тапсырманы іске қосу күйлерін және тапсырманы орындау нәтижелерін көруге болады.

- **Хабарландыру**

  Хабарландыру бөлімінде тапсырманы орындау нәтижелеріне қатысты оқиғаларды сақтау параметрлерін көрсетуге және тапсырманы орындау нәтижелері туралы хабарландыруларды конфигурациялауға болады.

- **Кесте**

  Кесте бөлімінде тапсырманы іске қосуға арналған кестені көрсетуге болады.

- **Мақсатты орны**

  Мақсатты орны бөлімінде Басқару сервері деректерінің сақтық көшірмелері сақталатын қалтаға апаратын жолды көрсетуге болады.

- **Параметрлер**

  Параметрлер бөлімінде деректердің сақтық көшірмесін жасау үшін құпиясөз қорғанысын және қажет болса, сақтық көшірмелердің санын орнатуға болады.

  Сондай-ақ, %ALLUSERSPROFILE% қалтасымен логикалық дискінің көлеңкелі көшірмесін жасауға және Басқару серверінің дерекқорын көшіруге болады. Мұны істеу үшін **Деректердің резервтік қоймасы үшін файлдық жүйенің суретін пайдалану** параметрін қосып, лездік суреттерді жасауға рұқсаты бар есептік жазбаның атауы мен құпиясөзін көрсетуіңіз керек.

- **Қауіпсіздік**

  Қауіпсіздік бөлімінде пайдаланушылар мен топтарға Басқару серверінде операцияларды орындау құқығын бере аласыз. **Басқару серверінен параметрлерді иелену** параметрі қосылса, тапсырманың қауіпсіздік параметрлері Басқару серверінен мұраға алынады.

  Бұл параметр өшірулі болса, сіз тапсырма параметрлерін конфигурациялай аласыз. Сіз пайдаланушыға немесе пайдаланушылар тобына рөл тағайындай аласыз немесе тапсырмаға қатысты тұрғыда пайдаланушыға немесе пайдаланушылар тобына құқықтар тағайындай аласыз.

  Әдепкі бойынша, **Басқару серверінен параметрлерді иелену** параметрі қосылады.

- **Тексерістер журналы**

  Тексерістер журналы бөлімінде тапсырма өзгерістерін бақылауға болады. Тапсырманың өзгерістерін сақтаған сайын, тексеру жасалады.

Деректерді сақтық көшірмелеу және қалпына келтіру утилитасы (klbackup)

Kaspersky Security Center дистрибутивінің құрамына кіретін klbackup утилитасы арқылы сақтық көшірмелеу және кейіннен қалпына келтіру үшін Басқару сервері деректерін көшіруге болады.

klbackup утилитасы екі режимде жұмыс істеуі мүмкін:

- интерактивті;
- тыныш.

Деректерді интерактивті режимде сақтық көшірмелеу және қалпына келтіру

Басқару сервері деректерін өзара әрекет режимінде klbackup утилитасын пайдалану арқылы жасалған сақтық көшірмеден қалпына келтіру кезінде қате пайда болуы мүмкін. Басқару сервері үшін 15.1.0.20748-pf2 патчын орнатқан болсаңыз, содан кейін **Дерекқорды көшіру** опциясы өшірілген klbackup утилитасын пайдаланып, сақтық көшірме жасасаңыз, осы көшірмені қалпына келтіру кезінде қате орын алады (MySQL және MariaDB қоспағанда барлық ДҚБЖ үшін). Басқару серверіне арналған 15.1.0.20748-pf2 патчы орнатылған болса және басқа ДҚБЖ-ға көшірместен сақтық көшірмені жасағыңыз келсе, деректердің сақтық көшірмесін жасау тапсырмасын пайдаланыңыз немесе пәрмен жолынан klbackup утилитасын іске қосыңыз.

Басқару сервері деректерін интерактивті режимде сақтық көшірмелеу үшін:

1. Kaspersky Security Center орнату қалтасында орналасқан klbackup утилитасын іске қосыңыз.

   Нәтижесінде, деректерді сақтық көшірмелеу және қалпына келтіру шебері іске қосылады.

2. Шебердің бірінші терезесінде **Басқару серверінің деректерін сақтық көшірмелеуді орындау** таңдаңыз.

   Тек Басқару серверінің сертификатын сақтық көшірмелеу немесе қалпына келтіру опциясын таңдасаңыз, басқару сервері сертификатының сақтық көшірмесі және жеке кілті ғана сақталады. Kaspersky Security Center Windows басқару серверін Kaspersky Security Center Linux басқару серверіне тасымалдаған кезде, басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасау пайдалы болуы мүмкін. Сондай-ақ басқарылатын құрылғыларды Kaspersky Security Center Linux басқару серверлері, сондай-ақ Kaspersky Security Center Windows басқару серверлері арасында тасымалдауға болады. Қосымша ақпарат алу үшін Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану бөлімін қараңыз.

   Келесі түймесін басыңыз.

3. Шебердің келесі терезесінде мына параметрлерді көрсетіңіз:

   - **Сақтық көшірменің межелі қалтасы**
   - **Дерекқорды көшіру**

     Басқару сервері деректерін қазіргі уақытта Microsoft SQL Server дерекқорында сақтасаңыз және оны келесі дерекқорлардың біріне көшіру қажет болса, бұл опцияны қосыңыз: MySQL немесе MariaDB, PostgreSQL немесе Postgres Pro, Azure SQL. Әдепкісінше бұл опция өшірулі.

     - **MySQL/MariaDB пішіміне көшіру**

       Қазіргі уақытта SQL Server серверін Басқару серверіне арналған ДҚБЖ ретінде қолдансаңыз және деректерді SQL Server серверінен MySQL немесе MariaDB серверіне тасымалдағыңыз келсе, осы параметрді қосыңыз. Kaspersky Security Center бағдарламасы MySQL және MariaDB серверімен үйлесімді деректердің сақтық көшірмесін жасайды. Осыдан кейін, сіз деректерді MySQL немесе MariaDB серверіндегі сақтық көшірмесінен қалпына келтіре аласыз.

- **Postgres-ке көшіру**

  Қазіргі уақытта SQL Server серверін басқару серверіне арналған ДҚБЖ ретінде қолдансаңыз және деректерді SQL Server серверінен PostgreSQL немесе Postgres Pro ДҚБЖ серверіне көшіргіңіз келсе, осы опцияны қосыңыз. Kaspersky Security Center қолданбасы PostgreSQL және Postgres Pro серверімен үйлесімді сақтық көшірме жасайды. Осыдан кейін деректерді сақтық көшірмеден PostgreSQL немесе Postgres Pro серверіне қалпына келтіре аласыз.

  Бұл опция Kaspersky техникалық қолдау қызметінен сұрасаңыз және басқару серверіне арналған 15.1.0.20748-pf2 патчын орнатсаңыз немесе Kaspersky Security Center Windows 15.1.0.22239 нұсқасына жаңартсаңыз қолжетімді болады.

- **Azure пішіміне ауысу**

  Қазіргі уақытта SQL Server серверін Басқару серверіне арналған ДҚБЖ ретінде қолдансаңыз және деректерді SQL Server серверінен Azure SQL серверіне тасымалдағыңыз келсе, осы параметрді қосыңыз. Kaspersky Security Center бағдарламасы Azure SQL серверімен үйлесімді деректердің сақтық көшірмесін жасайды. Осыдан кейін, сіз деректерді Azure SQL серверіндегі сақтық көшірмесінен қалпына келтіре аласыз.

- **Сақтық көшірменің мақсатты қалта атауында ағымдағы күн мен уақытты қосу**

- **Деректердің сақтық көшірмесіне арналған құпиясөз**

4. Сақтық көшірмелеуді орындау үшін **Келесі** түймесін басыңыз.

5. Amazon Web Services (AWS) немесе Microsoft Azure сияқты бұлтты ортадағы дерекқормен жұмыс істесеңіз, **Онлайн сақтау орнына кіру** терезесіндегі келесі өрістерді толтырыңыз:

   - AWS үшін:

     - **S3 орнының атауы**

       Деректердің сақтық көшірмесі үшін жасалған S3 орнының атауы.

     - **Қатынас кілтінің идентификаторы**

       Даналар қоймасындағы S3 орнымен жұмыс істеу үшін IAM пайдаланушысының есептік жазбасын жасаған кезде кілттің ID-ін (әріптер мен сандар бірізділігі) алдыңыз.

       Бұл өріс, S3 контейнеріне арналған RDS дерекқорын таңдаған кезде қолжетімді.

     - **Құпия кілт**

       IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

       Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

       Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

   - Microsoft Azure үшін:

     - **Azure сақтау орнының есептік жазба атауы**

       Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

- **Azure жазылым идентификаторы**

  Azure порталында жазылым жасадыңыз.

- **Azure құпиясөзі**

  Azure порталында бағдарламаның ID-ін жасау кезінде бағдарлама идентификаторына құпиясөз алдыңыз.

  Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

- **Azure бағдарламасының идентификаторы.**

  Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

  Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

- **Azure SQL сервері атауы**

  Көздің атауы мен тобы Azure SQL серверінің сипаттарында қолжетімді.

- **Azure SQL серверінің ресурстық тобы**

  Көздің атауы мен тобы Azure SQL серверінің сипаттарында қолжетімді.

- **Azure сақтау орнының қатынас кілті**

  "Access Keys" бөлімінде сақтаудың есептік жазбасы сипаттарында қолжетімді. Кез келген кілтті қолдана аласыз (key1 немесе key2).

Басқару серверінің деректерін интерактивті режимде қалпына келтіру үшін:

1. Kaspersky Security Center орнату қалтасында орналасқан klbackup утилитасын іске қосыңыз. Утилитаны Басқару сервері орнатылған есептік жазбамен іске қосыңыз. Утилитаны жаңа ғана орнатылған Басқару серверінде іске қосу ұсынылады.

   Нәтижесінде, деректерді сақтық көшірмелеу және қалпына келтіру шебері іске қосылады.

2. Шебердің бірінші терезесінде **Басқару серверінің деректерін қалпына келтіру** таңдап, **Келесі** түймесін басыңыз.

   Тек Басқару серверінің сертификатын сақтық көшірмелеу немесе қалпына келтіру опциясын таңдасаңыз, басқару сервері сертификаты мен жеке кілтін ғана қалпына келтіруге болады.

   Істен шығуға төзімді кластердің белсенді емес түйінінде klbackup утилитасын іске қосқан кезде сізден нұсқалардың бірін таңдау сұралады: Басқару сервері сертификатын көрсету немесе Басқару серверінен деректерді автоматты түрде алу.

3. **Қалпына келтіру параметрлері** шебері терезесінде:

   - Басқару сервері деректерінің сақтық көшірмесі бар қалтаны көрсетіңіз.

     AWS немесе Azure сияқты бұлтты ортада жұмыс істесеңіз, сақтау орнының мекенжайын көрсетіңіз. Файлдың атауы backup.zip екеніне де көз жеткізіңіз.

- Деректерді сақтық көшірмелеу кезінде енгізілген құпиясөзді көрсетіңіз.

  Деректерді қалпына келтіру кезінде, сақтық көшірмелеу барысында енгізілген құпиясөзді көрсету қажет. Сақтық көшірмелеуден кейін ортақ қатынасы бар қалтаға апаратын жол өзгерсе, қалпына келтірілген деректерді пайдаланатын тапсырмалардың жұмысын тексеріңіз (қалпына келтіру тапсырмалары және қашықтан орнату тапсырмалары). Қажет болса, осы тапсырмалардың параметрлерін өңдеңіз. Деректер сақтық көшірме файлынан қалпына келтіріліп жатқанда, ешкім Басқару серверінің ортақ қатынасы бар қалтасына кіре алмайды. klbackup утилитасы іске қосылатын есептік жазба ортақ қатынасы бар қалтаға толық қатынасу мүмкіндігіне ие болуы керек.

4. Деректерді қалпына келтіру үшін **Келесі** түймесін басыңыз.

Деректерді тыныш режимде сақтық көшірмелеу және қалпына келтіру

Деректерді сақтық көшірмелеу немесе Басқару сервері деректерін тыныш режимде қалпына келтіру үшін,

Басқару сервері орнатылған құрылғының пәрмен жолында klbackup утилитасын қажетті кілттер жиынтығымен іске қосыңыз.

klbackup утилитасын пайдаланған кезде, желілік агент жалаушалары қалпына келтірілмейді. Желілік агент жалаушаларын қолмен конфигурациялау қажет.

Қалпына келтіру әрекеті орындалатын басқару серверінің данасында бір түрдегі ДҚБЖ қолданылуы керек. Басқару серверінің нұсқасы сондай (ұқсас немесе барынша жаңа патчпен) немесе барынша жаңа болуы мүмкін.

Утилитаның пәрмен жолының синтаксисі:

```
klbackup -path <backup path> [-linux_path < SQL Server backup path >][-node_cert
< сертификат жолы >] [-logfile < журнал файлы >] [-use_ts]|[-restore] [-password
< құпиясөз >] [-cert_only] [-online] [-migrate postgres]
```

Егер сіз klbackup утилитасының пәрмен жолында құпиясөзді белгілемесеңіз, утилита оны интерактивті түрде енгізуді сұрайды.

Кілттердің сипаттамалары:

- `-path <сақтық көшірме жолы>` — көрсетілген сақтық көшірме қалтасындағы ақпаратты сақтаңыз немесе қалпына келтіру үшін сақтық көшірме қалтасындағы деректерді пайдаланыңыз (міндетті параметр).

  Дерекқор серверінің есептік жазбасы және klbackup утилитасы сақтық көшірме қалтасындағы деректерді өзгерту құқығына ие болуы керек.

- `-linux_path <SQL Server backup path>` – Linux жүйесіне арналған SQL Server үшін деректердің сақтық көшірмесі бар қалтаның жергілікті жолы.

  Дерекқор серверінің есептік жазбасы және klbackup утилитасы SQL Server сақтық көшірме қалтасындағы деректерді өзгерту құқығына ие болуы керек.

- `-node_cert <сертификат жолы>` — қалпына келтіруден кейін белсенді емес ақауларға төзімді түйінді конфигурациялауға арналған сервер сертификатының файлы. Параметр көрсетілмесе, ол серверден автоматты түрде алынады.

  Істен шығуға төзімді кластердің белсенді емес түйінінде klbackup утилитасын іске қосқан кезде, осы пернені Басқару сервері сертификатына жолды көрсету үшін пайдаланыңыз.

- `-logfile <журнал файлы>` — басқару сервері деректерінің сақтық көшірмесін жасау немесе қалпына келтіру туралы есепті сақтау.

- `-use_ts` — деректерді сақтаған кезде, ақпаратты сақтық көшірме қалтасына, `klbackup YYYY-MM-DD # HH-MM-SS` форматымен аталатын ішкі қалтаға көшіріңіз. Онда ағымдағы күн мен операция уақыты (UTC) қамтылған. Кілт көрсетілмеген болса, ақпарат сақтық көшірме қалтасының түбірінде сақталады.

  Ақпаратты сақтық көшірмесі бар қалтаға сақтауға тырысқанда, қате туралы хабар пайда болады. Ақпарат жаңартылмайды.

  `-use_ts` кілтінің болуы арқасында Басқару сервері деректері мұрағатын жүргізуге болады. Мысалы, егер `-path` кілтімен `C:\KLBackups` қалтасы жасалған болса, онда `klbackup 2022-06-19 # 11-30-18` қалтасында Басқару серверінің 2022 жылғы 19 маусым, 11 сағат 30 минут 18 секундтағы күйі туралы ақпарат сақталады.

- `-restore` – Басқару сервері деректерін қалпына келтіруді орындау. Деректерді қалпына келтіру сақтық көшірме қалтасында ұсынылған ақпарат негізінде жүзеге асырылады. Кілт болмаса, сақтық көшірме қалтасына деректердің сақтық көшірмесі жасалады.

- `-password <құпиясөз>` — құпия деректерді қорғауға арналған құпиясөз.

  > Ұмытылған құпиясөзді қалпына келтіру мүмкін емес. Құпиясөзге қойылатын талаптар жоқ. Құпиясөздің ұзындығы шектелмейді, сондай-ақ құпиясөздің нөлдік ұзындығы да болуы мүмкін (яғни құпиясөзсіз).

  Деректерді қалпына келтіру кезінде, сақтық көшірмелеу барысында енгізілген құпиясөзді көрсету қажет. Сақтық көшірмелеуден кейін ортақ қатынасы бар қалтаға апаратын жол өзгерсе, қалпына келтірілген деректерді пайдаланатын тапсырмалардың жұмысын тексеріңіз (қалпына келтіру тапсырмалары және қашықтан орнату тапсырмалары). Қажет болса, осы тапсырмалардың параметрлерін өңдеңіз. Деректер сақтық көшірме файлынан қалпына келтіріліп жатқанда, ешкім Басқару серверінің ортақ қатынасы бар қалтасына кіре алмайды. klbackup утилитасы іске қосылатын есептік жазба ортақ қатынасы бар қалтаға толық қатынасу мүмкіндігіне ие болуы керек. Утилитаны жаңа ғана орнатылған Басқару серверінде іске қосу ұсынылады.

- `-cert_only` – Басқару серверінің сертификаты мен жеке кілтін ғана сақтау немесе қалпына келтіру.

  Бұл жалауша Kaspersky Security Center Windows басқару серверінен Kaspersky Security Center Linux бсқару серверіне тасымалдау әрекетін орындаған кезде пайдалы болуы мүмкін. Сондай-ақ Kaspersky Security Center Linux басқару серверлері, сонымен қатар Kaspersky Security Center Windows басқару серверлері арасында басқарылатын құрылғыларды тасымалдауға болады.

- `-online` – Басқару серверінің автономды күйінің уақытын барынша азайту үшін лездік сурет жасау арқылы Басқару сервері деректерінің сақтық көшірмесін жасау. Егер сіз деректерді сақтық көшірмелеу және қалпына келтіру утилитасын қолдансаңыз, бұл параметр еленбейді. Басқа ДҚБЖ көшіру үшін сақтық көшірме жасау кезінде бұл жалаушаны пайдаланбаңыз.

- `-archive 0` — сервер деректерін кәдімгі файлдар ретінде сақтаңыз. Әдепкісінше (`-archive 1`) сервер деректері мұрағат файлында сақталады.

- `-migrate mysql` — SQL Server дерекқорында сақталған, MySQL-мен (соның ішінде MariaDB) үйлесімді басқару сервері деректерінің сақтық көшірмесін жасаңыз. Деректерді сақтық көшірмеден MySQL серверіне қалпына келтіре аласыз.

- `-migrate postgres` — SQL Server дерекқорында сақталған, PostgreSQL және Postgres Pro-мен үйлесімді басқару сервері деректерінің сақтық көшірмесін жасаңыз. Деректерді сақтық көшірмеден PostgreSQL немесе Postgres Pro ішіне қалпына келтіруге болады. Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы Kaspersky Security Center Linux жүйесіне көшірген кезде осы жалаушаны пайдаланыңыз.

  Бұл опция Kaspersky техникалық қолдау қызметінен сұрасаңыз және басқару серверіне арналған 15.1.0.20748-pf2 патчын орнатсаңыз немесе Kaspersky Security Center Windows 15.1.0.22239 нұсқасына жаңартсаңыз қолжетімді болады.

Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану

klbackup утилитасы басқа басқару серверінің басқаруындағы басқарылатын құрылғыларды ауыстыруға мүмкіндік береді. Тасымалдау әрекетін орындаған кезде, Kaspersky Security Center Windows басқару серверін Kaspersky Security Center Linux басқару серверіне klbackup утилитасы көмегімен өзгертуге болады. Сондай-ақ басқарылатын құрылғыларды Kaspersky Security Center Linux басқару серверлері, сондай-ақ Kaspersky Security Center Windows басқару серверлері арасында тасымалдауға болады.

klbackup утилитасы көмегімен басқа басқару серверінің басқаруындағы басқарылатын құрылғыларды ауыстыру үшін:

1. Алдыңғы құрылғыда басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасаңыз.

   Сақтық көшірмені келесі жолдардың бірімен жасауға болады:

   - klbackup утилитасының интерфейсін пайдалану арқылы (тек Kaspersky Security Center Windows басқару сервері үшін)

     Kaspersky Security Center орнату қалтасындағы klbackup утилитасын іске қосыңыз, содан кейін **Тек Басқару серверінің сертификатын сақтық көшірмелеу немесе қалпына келтіру** опциясы көмегімен сақтық көшірме жасаңыз.

   - Пәрмен нұсқауын пайдалану арқылы (Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлерінің 15.1 немесе одан кейінгі нұсқасы үшін)

     Басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасау үшін пәрмен жолындағы `-cert_only` кілтімен klbackup утилитасын іске қосыңыз.

     ```
     klbackup -path <басқару сервері сертификатының сақтық көшірмесіне апаратын жол> -cert_only
     ```

2. Алдыңғы құрылғыда басқару серверін желіден ажыратыңыз.

3. Құрылғыға басқа басқару серверіндегідей мекенжайды тағайындаңыз.

   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk қызметтік бағдарламасын қолданып, басқарылатын құрылғыларда алуға болады).

4. Басқа басқару сервері бар құрылғыда сақтық көшірмеден басқару серверінің сертификатын және жеке кілтті қалпына келтіріңіз.

   Сақтық көшірмені келесі жолдардың бірімен қалпына келтіруге болады:

   - klbackup утилитасының интерфейсін пайдалану арқылы (тек Kaspersky Security Center Windows басқару сервері үшін)

     klbackup утилитасын іске қосыңыз, содан кейін **Тек Басқару серверінің сертификатын сақтық көшірмелеу немесе қалпына келтіру** опциясы көмегімен сақтық көшірмені қалпына келтіріңіз.

- Пәрмен нұсқауын пайдалану арқылы (Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлерінің 15.1 немесе одан кейінгі нұсқасы үшін)

  Басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін қалпына келтіру үшін пәрмен жолындағы `-cert_only` кілтімен klbackup утилитасын іске қосыңыз.

  ```
  klbackup -path <басқару сервері сертификатының сақтық көшірмесіне апаратын жол> -restore -cert_only
  ```

Басқарылатын құрылғылар басқа басқару серверінің басқаруына тапсырылады. Осы басқару серверіне өтіп, басқарылатын құрылғылардың желіде көрінетініне және желілік агент орнатылып, оларда жұмыс істейтініне көз жеткізуге болады (**Көзге көрінетін** опциясындағы *Иә* мәні, **Желілік агент орнатылған** және **Желілік агент іске қосулы** бағандары).

MySQL немесе MariaDB пайдалану кезінде басқару сервері деректерінің сақтық көшірмесін жасау және қалпына келтіру

Басқару сервері деректерін Kaspersky Security Center Linux басқаруындағы Kaspersky Security Center Windows жүйесінен тасымалдау үшін деректердің сақтық көшірмесін пайдалануға болады. Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы тасымалдау әрекетіне Kaspersky Security Center Windows жүйесінің кез келген қолдау көрсетілетін нұсқасынан Kaspersky Security Center Linux 15.2 немесе одан кейінгі нұсқасына тасымалдау арқылы ғана қолдау көрсетіледі.

Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін ДҚБЖ ретінде MySQL немесе MariaDB жүйесін пайдалансаңыз, `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ үшін сәйкес келуі керек. Әйтпесе басқару серверінің деректері қате тасымалданады.

Kaspersky Security Center Windows жүйесінде басқару сервері деректерінің сақтық көшірмесін жасамай тұрып, `lower_case_table_names` параметрінің мәнін тексеріңіз. ДҚБЖ орнату кезінде бұл параметрді бұрын көрсетпесеңіз, әдепкі параметр мәні пайдаланылады. Windows жүйесіне арналған `lower_case_table_names` параметрінің әдепкі мәні — `1`.

Kaspersky Security Center Linux жүйесіне арналған MySQL немесе MariaDB орнату кезінде MySQL веб-сайтындағы нұсқауды пайдаланып, `lower_case_table_names` параметрін Windows жүйесіне арналған осы параметр үшін көрсетілген мәнге орнатыңыз. Бұл параметрді көрсетпесеңіз, әдепкі параметр мәні пайдаланылады. Linux негізіндегі операциялық жүйелер үшін `lower_case_table_names` параметрінің әдепкі мәні Windows жүйесіне арналған әдепкі мәннен өзгеше.

MySQL 8.0 орнатқыңыз келсе, осы нұсқауға сәйкес `lower_case_table_names` параметрін көрсету жұмыс істемеуі мүмкін. Бұл жағдайда алдымен MySQL 5.7 орнатуыңыз керек, нұсқауды пайдаланып, `lower_case_table_names` параметрін көрсетіңіз, содан кейін MySQL 5.7 нұсқасын MySQL 8.0 нұсқасына жаңартыңыз. `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ-ларға сәйкес келмесе, басқару серверінің деректері дұрыс қалпына келтірілмейді.

Басқару сервері деректерінің сақтық көшірмесін жасау мен қалпына келтіруді оңтайландыру

Басқару серверінің іркілісін азайту мақсатында басқару сервері деректерінің сақтық көшірмесін жасау мен қалпына келтіруді оңтайландыру үшін келесі әрекеттердің бірін орындаңыз:

- **Деректердің сақтық көшірмесін жасау үшін файлдық жүйе снапшотын пайдалану** опциясын қосу.

  Мәліметтер алу үшін келесі мақаланы қараңыз: Сақтық көшірме жасау уақытын азайту үшін файлдық жүйе снапшотын пайдалану.

- Келесі жалаушаларды конфигурациялаңыз:

  Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

  - `KLSRV_BKP_FILES` — дерекқор файлын 2-ден 32-ге дейінгі бірнеше кішірек файлға бөледі. Бұл жағдайда ДҚБЖ өнімділігіне процессор шектеу қойған кезде сақтық көшірме жасау мен қалпына келтіру процесі жеделдейді.

    Мысалы:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS` — `COMPRESSION` және `MAXTRANSFERSIZE` параметрлерін көрсетеді. Бұл жағдайда ДҚБЖ өнімділігіне файл кірісі/шығысы шектеу қойған кезде сақтық көшірме жасау процесі жеделдейді.

    Мысалы:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS` — `MAXTRANSFERSIZE` параметрін көрсетеді. Бұл жағдайда ДҚБЖ өнімділігіне файл кірісі/шығысы шектеу қойған кезде қалпына келтіру процесі жеделдейді.

    Мысалы:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
    = 4194304"
    ```

  - `KLSRV_BKP_ONLINE_DB_BACKUP` — сақтық көшірме жасау кезінде басқару серверінің кідіріс уақытын жояды. Тек келесі ДҚБЖ-лар үшін қолжетімді:

    - PostgreSQL, Postgres Pro.
    - Толық қалпына келтіру үлгісі бар SQL сервері. Мәліметтер алу үшін SQL серверінің құжаттамасын қараңыз. `KLSRV_BKP_ONLINE_DB_BACKUP` жалаушасын қосқанда, SQL серверінің ДҚБЖ-сы толық қалпына келтіру үлгісіне автоматты түрде ауысады.

    Мысалы:

    ```
    klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
    ```

Басқару серверін басқа құрылғыға тасымалдау

Егер сізге жаңа құрылғыда Басқару серверін пайдалану қажет болса, оны келесі тәсілдердің бірімен тасымалдауға болады:

- Басқару серверін және дерекқор серверін жаңа құрылғыға жылжытыңыз (дерекқор серверін жаңа құрылғыға басқару серверімен бірге немесе басқа құрылғыға орнатуға болады).
- Дерекқор серверін ескі құрылғыда қалдыру және жаңа құрылғыға тек Басқару серверін тасымалдау.

Басқару серверін жаңа құрылғыға тасымалдау үшін:

1. Алдыңғы құрылғыда Басқару сервері деректерінің сақтық көшірмесін жасаңыз.

   Бұл үшін, Басқару консолінің көмегімен деректерді сақтық көшірмелеу тапсырмасын іске қосыңыз немесе klbackup утилитасын іске қосыңыз.

Егер сіз SQL Server серверін Басқару сервері үшін ДҚБЖ ретінде қолдансаңыз, деректерді SQL Server серверінен MySQL немесе MariaDB ДҚБЖ жүйесіне тасымалдауға болады. Деректерді сақтық көшірмелеу үшін klbackup утилитасын интерактивті режимде іске қосыңыз. Сақтық көшірмелеу және деректерді қалпына келтіру шеберінің **Сақтық көшірмелеу параметрлері** терезесінде **MySQL/MariaDB пішіміне көшіру** параметрін қосыңыз. Kaspersky Security Center бағдарламасы MySQL және MariaDB серверімен үйлесімді деректердің сақтық көшірмесін жасайды. Осыдан кейін, сіз деректерді MySQL немесе MariaDB серверіндегі сақтық көшірмесінен қалпына келтіре аласыз.

Сондай-ақ, деректерді SQL Server серверінен Azure SQL ДҚБЖ жүйесіне тасымалдағыңыз келсе, **Azure пішіміне ауысу** параметрін қосуға болады.

2. Алдыңғы құрылғыда басқару серверін желіден ажыратыңыз.

3. Басқару сервері орнатылатын жаңа құрылғыны таңдаңыз. Таңдалған құрылғыдағы аппараттық және бағдарламалық жасақтама Басқару серверіне, Басқару консоліне және Желілік агентке қойылатын талаптарға сәйкес келетініне көз жеткізіңіз. Басқару серверінде қолданылатын порттардың қолжетімді екеніне көз жеткізіңіз.

4. Жаңа құрылғыға сол мекенжайды тағайындаңыз.

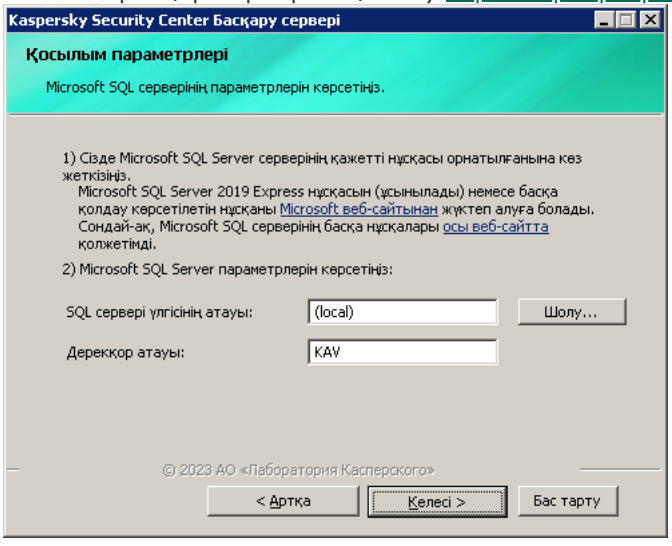
   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk қызметтік бағдарламасын қолданып, басқарылатын құрылғыларда алуға болады).

5. Қажет болса, жаңа құрылғыда басқару сервері пайдаланатын дерекқорларды басқару жүйесін (ДҚБЖ) орнатыңыз.

   Дерекқорды басқару серверімен бірге жаңа құрылғыға немесе басқа құрылғыға орнатуға болады. Таңдалған құрылғы аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз. ДҚБЖ таңдау кезінде Басқару сервері қызмет көрсететін құрылғылардың санын ескеріңіз.

6. Жаңа құрылғыда басқару серверінің орнатылымын іске қосыңыз.

7. Басқару серверін орнатқан кезде, дерекқор серверіне қосылу параметрлерін реттеңіз.



Microsoft SQL Server үшін қосылым параметрлері терезесінің мысалы

Дерекқор серверін қайда орналастыру керек екеніне байланысты, келесі әрекеттердің бірін орындаңыз:

- **Алдыңғы құрылғыда дерекқор серверін қалдырыңыз.**

  1. **SQL сервері үлгісінің атауы** өрісінің жанында **Шолу** түймесін басыңыз және пайда болған тізімде алдыңғы құрылғының атауын таңдаңыз.

     Алдыңғы құрылғы жаңа Басқару серверімен байланысу үшін қолжетімді болуы керек екенін ескеріңіз.

  2. **Дерекқор атауы** өрісінде алдыңғы дерекқор атауын енгізіңіз.

- **Дерекқор серверін басқа құрылғыға жылжытыңыз.**

  1. **SQL сервері үлгісінің атауы** өрісінің жанында **Шолу** түймесін басыңыз және пайда болған тізімде құрылғы атауын таңдаңыз.

  2. **Дерекқор атауы** өрісінде жаңа дерекқор атауын енгізіңіз.

     Жаңа дерекқордың атауы алдыңғы құрылғыдағы дерекқордың атауына сәйкес келуі керек екенін ескеріңіз. Басқару серверінің сақтық көшірмесін пайдалану үшін дерекқорлардың атауы сәйкес келуі керек. Дерекқордың әдепкі бойынша атауы *KAV*.

8. Орнату аяқталғаннан кейін, klbackup утилитасын көмегімен жаңа құрылғыдағы Басқару сервері деректерін қалпына келтіріңіз.

   Егер сіз SQL Server серверін алдыңғы және жаңа құрылғыларда ДҚБЖ ретінде қолдансаңыз, жаңа құрылғыда орнатылған SQL Server нұсқасы алдыңғы құрылғыда орнатылған SQL Server нұсқасымен бірдей немесе одан жоғары болуы керек екенін ескеріңіз. Әйтпесе, сіз жаңа құрылғыдағы Басқару сервері деректерін қалпына келтіре алмайсыз.

9. Басқару консолін ашып, Басқару серверіне қосылыңыз.

10. Барлық басқарылатын құрылғылар басқару серверіне қосылғанына көз жеткізіңіз.

11. Алдыңғы құрылғыдан Басқару сервері мен дерекқорлар серверін жойыңыз.

Kaspersky Security Center Web Console веб-консолін Басқару сервері мен дерекқорлар серверін басқа құрылғыға тасымалдау үшін де пайдалануға болады.

Басқару серверлері арасындағы қақтығыстардан аулақ болу

Егер желіде бірнеше Басқару сервері болса, олар бірдей клиент құрылғыларын көре алады. Бұл, мысалы, басқару серверінің басқа басқару сервері орнатқан қолданбаны орнатуына және басқа қайшылықтарға әкелуі мүмкін. Қолданбаның басқа басқару сервері басқаратын құрылғыға орнатылуына жол бермеу үшін **Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату** тапсырма сипаттарындағы *Бағдарламаны қашықтан орнату* опциясын қосу керек.

Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату опциясын қоссаңыз, содан кейін *Бағдарламаны қашықтан орнату* тапсырмасын іске қоссаңыз, құрылғылардың басқа басқару сервері арқылы басқарылатынын анықтау үшін тексеру орындалады. Басқа басқару сервері басқаратын құрылғылар үшін **Басқа Басқару серверімен басқарылады** төлсипаты `true` мәніне орнатылады. *Бағдарламаны қашықтан орнату* тапсырмасы бұл құрылғыларға қолданылмайды.

Басқа Басқару серверімен басқарылады төлсипат мәндері басқарылатын құрылғылар тізіміндегі және тағайындалмаған құрылғылар тізіміндегі **Басқа Басқару серверімен басқарылады** бағанында көрсетіледі.

Басқа Басқару серверімен басқарылады сипаты келесі операцияларға арналған өлшемшарт ретінде де қолданылуы мүмкін:

- Құрылғыларды іздеу
- Құрылғыны таңдаулары
- Құрылғыны жылжыту ережелері
- Автоматты түрде тег қою ережелері

Басқа Басқару серверімен басқарылады атрибутын қалпына келтіру үшін:

1. Kaspersky Security Center Web Console негізгі мәзірінде **Табу және орналастыру** → **Тағайындалмаған құрылғылар** тармағына өтіңіз.
2. Қажетті құрылғыны таңдап, **Басқа Басқару сервері арқылы басқарылатын атрибутты өшіру** түймесін басыңыз.

Басқа Басқару серверімен басқарылады төлсипаты қалпына келтірілді.

Басқару топтарын басқару

Бұл бөлімде басқару топтарымен жұмыс істеу туралы ақпарат бар.

Басқару топтарымен келесі әрекеттерді орындауға болады:

- басқару тобының құрамына иерархияның кез келген деңгейлеріндегі салынған топтардың ерікті санын қосу;
- құрылғының басқару топтарының құрамына қосу;
- жеке құрылғыларды және тұтас топтарды басқа топтарға жылжыту арқылы басқару топтарының иерархиясын өзгерту;
- басқару топтарының құрамынан салынған топтар мен құрылғыларды жою;
- басқару топтарына қосалқы және виртуалды Басқару серверлерін қосу;
- құрылғыларды бір Сервердің басқару топтары құрамынан басқа Сервердің басқа топтарына тасымалдау;
- Kaspersky қандай бағдарламалары топ құрамына қосылатын құрылғыларға автоматты түрде орнатылатынын анықтаңыз.

Басқарғыңыз келетін басқару топтарына (немесе осы топтар тиесілі басқару серверіне) арналған **Басқару топтарын басқару** аймағында **Өзгерту** рұқсаты болса ғана, бұл әрекеттерді орындай аласыз.

Басқару топтарын жасау

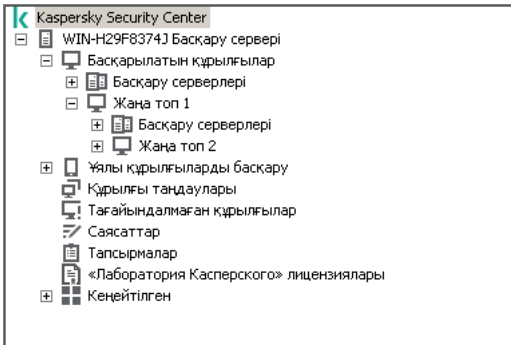
Басқару топтары иерархиясы Kaspersky Security Center бағдарламасының басты терезесінде, **Басқарылатын құрылғылар** қалтасында қалыптастырылады. Басқару топтары консоль тармағында қалталар ретінде көрсетіледі (төмендегі суретті қараңыз).

Kaspersky Security Center бағдарламасы орнатылғаннан кейін, **Басқарылатын құрылғылар** қалтасы бірден бос **Басқару серверлері** қалтасын ғана қамтиды.

Консоль ағашында **Басқару серверлері** қалтасының болуы немесе болмауы пайдаланушы интерфейсі параметрлері тарапынан анықталады. Осы қалтасының көрсетілуін қосу үшін **Көру → Интерфейсті конфигурациялау** мәзіріне өтіп, ашылған **Интерфейсті конфигурациялау** терезесінде **Қосалқы Басқару серверлерін көрсету** жалаушасын қою керек.

Басқару топтарының иерархиясын құру кезінде **Басқарылатын құрылғылар** қалтасына құрылғылар мен виртуалды машиналарды қосып, салынған топтарды қосуға болады. **Басқару серверлері** қалтасына қосалқы және виртуалды Басқару серверлерін қосуға болады.

Басқарылатын құрылғылар қалтасы сияқты, әрбір жасалған топ, алдымен осы топтың қосалқы және виртуалды Басқару серверлерімен жұмыс істеу үшін бос **Басқару серверлері** қалтасын ғана қамтиды. Осы топтың саясаты мен тапсырмалары туралы ақпарат, сондай-ақ осы топқа кіретін құрылғылар туралы ақпарат сол топтың жұмыс аймағындағы тиісті атаулары бар қойыншаларда көрсетіледі.



Басқару топтарының иерархиясын қарау

Басқару тобын жасау үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын ашыңыз.

2. Егер сіз бұрыннан бар басқару тобының ішкі тобын құрғыңыз келсе, **Басқарылатын құрылғылар** қалтасында жаңа басқару тобы кіруі тиісті топқа сәйкес келетін салынған қалтаны таңдаңыз.

   Егер сіз иерархияның жоғарғы деңгейінің жаңа басқару тобын құрсаңыз, бұл қадамды өткізіп жіберуге болады.

3. Басқару тобын жасау процесін келесі тәсілдердің бірімен іске қосыңыз:

   - **Жасау** → **Топ** контекстік мәзірі пәрменінің көмегімен;
   - **Құрылғылар** қойыншасындағы бағдарламаның басты терезенің жұмыс аймағында орналасқан **Жаңа топ** түймесі арқылы.

4. Ашылған **Топ атауы** терезесінде топтың атауын енгізіп, **OK** түймесін басыңыз.

Нәтижесінде, консоль ағашында берілген атауы бар жаңа басқару тобы қалтасы пайда болады.

Бағдарлама Active Directory құрылымына немесе домендік желі құрылымына негізделген басқару топтарының құрылымын құруға мүмкіндік береді. Сондай-ақ, мәтіндік файлдан топтар құрылымын жасауға болады.

Басқару топтарының құрылымын құру үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
2. **Басқарылатын құрылғылар** қалтасының мәнмәтіндік мәзірінде **Барлық тапсырмалар** → **Жаңа топ құрылымы** тармағын таңдаңыз.

Нәтижесінде, басқару топтарының құрылымын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Басқару топтарын жылжыту

Салынған басқару топтарын топтар иерархиясының ішінде жылжытуға болады.

Басқару тобы барлық салынған топтармен, қосалқы Басқару серверлерімен, құрылғылармен, топтық саясаттармен және тапсырмалармен бірге жылжытылады. Оған басқару топтарының иерархиясындағы жаңа жайғасымына сәйкес келетін барлық параметрлер қолданылады.

Топ атауы иерархияның бір деңгейінде бірегей болуы керек. Сіз басқару тобын жылжытып жатқан қалтада ұқсас атауы бар топ бұрыннан болса, жылжытпас бұрын топтың атауын өзгерту керек. Жылжытылатын топтың атауын алдын ала өзгертпеген болсаңыз, жылжыту кезінде оның атауына автоматты түрде түр **(<реттік нөмір>)** жалғауы, мысалы: **(1)**, **(2)** қосылады.

Басқарылатын құрылғылар тобының атауын өзгерту мүмкін емес, себебі ол Басқару консолінің кіріктірілген элементі болып табылады.

Топты консоль ағашының басқа қалтасына жылжыту үшін:

1. Консоль ағашында жылжытылатын топты таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:

   - Контекстік мәзір арқылы топты жылжытыңыз:

     1. Топтың контекстік мәзірінде **Қию** тармағын таңдаңыз;
     2. Таңдалған топты жылжыту қажет басқару тобының контекстік мәзірінен **Кірістіру** тармағын таңдаңыз.

- Бағдарламаның бас мәзірі арқылы топты жылжытыңыз:

  a. Бас мәзірдің **Әрекет** → **Қию** тармағын таңдаңыз.

  b. Консоль ағашында, таңдалған топты жылжыту қажет басқару тобын таңдаңыз.

  c. Бас мәзірдің **Әрекет** → **Салу** тармағын таңдаңыз.

- Тінтуірдің көмегімен топты консоль ағашындағы басқа топқа жылжытыңыз.

Басқару топтарын жою

Басқару тобында қосалқы Басқару серверлері, салынған топтар және клиент құрылғылары болмаса және ол үшін тапсырмалар мен саясаттар қалыптастырылмаса, сіз бұл басқару тобын жоя аласыз.

Басқару тобын жоймас бұрын, оның құрамынан қосалқы Басқару серверінен, салынған топтарды және клиент құрылғыларын жою қажет.

Топты жою үшін:

1. Консоль ағашында басқару топтарын таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:

   - топтың контекстік мәзірінде **Жою** тармағын таңдаңыз;
   - бағдарламаның бас мәзірінде **Әрекет** → **Жою** тармағын таңдаңыз;
   - **DELETE** түймесін басыңыз.

Басқару топтарының құрылымын автоматты түрде жасау

Kaspersky Security Center бағдарламасы топтар құрылымын жасау шеберінің көмегімен басқару топтарының құрылымын автоматты түрде қалыптастыруға мүмкіндік береді.

Шебер келесі деректер негізінде басқару топтарының құрылымын жасайды:

- Windows желісінің жұмыс топтары мен домендерінің құрылымы;
- Active Directory топтары құрылымы;
- әкімші қолмен жасаған мәтіндік файлдың мазмұны.

Мәтіндік файлды қалыптастыру кезінде келесі ережелерді ұстану керек:

- Әрбір жаңа топтың атауы жаңа жолдан басталуы тиіс: бөлгіш жол үзігінен басталуы керек. Бос жолдар еленбейді.

  Мысалы:

  Кеңсе 1

  Кеңсе 2

  Кеңсе 3

  Мақсатты топта бірінші иерархия тобының үш тобы құрылады.

- Салынған топтың атауын қисық сызық (/) арқылы көрсету керек.

  Мысалы:

  Кеңсе 1/Бөлімше 1/Бөлім 1/Топ 1

  Мақсатты топта бір-біріне салынған төрт ішкі топ құрылады.

- Иерархия деңгейі бірдей болатын бірнеше салынған топты құру үшін "топқа апаратын толық жолды" көрсету керек.

  Мысалы:

  Кеңсе 1/Бөлімше 1/Бөлім 1

  Кеңсе 1/Бөлімше 2/Бөлім 1

  Кеңсе 1/Бөлімше 3/Бөлім 1

  Кеңсе 1/Бөлімше 4/Бөлім 1

  Мақсатты топта "Кеңсе 1" бірінші иерархия деңгейінің бір тобы құрылып, оның құрамына иерархия деңгейі бірдей болатын төрт салынған топ кіреді: "Бөлімше 1", "Бөлімше 2", "Бөлімше 3" және "Бөлімше 4". Осы топтардың әрқайсысының құрамына "Бөлім 1" тобы кіретін болады.

Шебердің көмегімен басқару топтарының құрылымын құру кезінде желінің бүтіндігі бұзылмайды: жаңа топтар қолданыстағы топтарды алмастырмайды, тек қосылады. Клиент құрылғысы басқару тобының құрамына қайтадан қосыла алмайды, себебі құрылғыны басқару тобына көшіру кезінде ол **Тағайындалмаған құрылғылар** тобына жойылады.

Басқару топтарының құрылымын құру кезінде құрылғы қандай да бір себептермен **Тағайындалмаған құрылғылар** тобының құрамына қосылмай қалған (өшірілген, желіден ажыратылған) болса, ол басқару тобына автоматты түрде көшірілмейді. Шебердің жұмысы аяқталғаннан кейін, құрылғыларды басқару топтарына қолмен қоса аласыз.

Басқару топтарының құрылымын автоматты түрде жасауды іске қосу үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
2. **Басқарылатын құрылғылар** қалтасының мәнмәтіндік мәзірінде **Барлық тапсырмалар → Жаңа топ құрылымы** тармағын таңдаңыз.

   Нәтижесінде, басқару топтарының құрылымын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Бағдарламаларды басқару тобының құрылғыларына автоматты түрде орнату

Басқару тобында Kaspersky қолданбасын клиент құрылғыларына автоматты түрде қашықтан орнату үшін қолданылатын орнату пакеттерін көрсетуге болады.

Қолданбаларды басқару тобының құрылғыларына автоматты түрде орнатуды конфигурациялау үшін:

1. Консоль ағашынан қажетті басқару тобын таңдаңыз.
2. Осы басқару тобының сипаттар терезесін ашыңыз.
3. **Бөлімдер** панеліндегі **Автоматты орнату** опциясын таңдап, жұмыс аймағында құрылғыларда орнатылатын қолданбалардың орнату пакеттерін таңдаңыз.
4. **OK** түймесін басыңыз.

Топтық тапсырмалар жасалды. Бұл тапсырмалар клиент құрылғыларында басқару тобына қосылғаннан кейін бірден іске қосылады.

Егер автоматты түрде орнату үшін бір бағдарламаның бірнеше орнату пакеттері көрсетілсе, орнату тапсырмасы тек бағдарламаның соңғы нұсқасы үшін жасалады.

Клиент құрылғыларын басқару

Бұл бөлімде клиент құрылғыларымен жұмыс істеу туралы ақпарат бар.

Клиент құрылғыларын Басқару серверіне қосу

Клиент құрылғысын Басқару серверіне қосуды клиент құрылғысында орнатылған Желілік агент жүзеге асырады.

Клиент құрылғысын Басқару серверіне қосқан кезде келесі операциялар орындалады:

- Деректерді автоматты түрде синхрондау:
  - клиент құрылғысында орнатылған бағдарламалар тізімін синхрондау;
  - саясаттарды, бағдарлама параметрлерін, тапсырмаларды және тапсырма параметрлерін синхрондау.
- Сервердің бағдарламалардың күйі, тапсырмалардың орындалуы және бағдарламалардың жұмыс статистикасы туралы ағымдағы ақпаратты алуы.
- Өңдеуді қажет ететін оқиғалар туралы ақпаратты Серверге жеткізу.

Деректерді автоматты түрде синхрондау Желілік агенттің параметрлеріне сәйкес мезгіл-мезгіл жасалады (мысалы, 15 минутта бір рет). Қосылымдар арасындағы аралықты қолмен белгілеуге болады.

Оқиға туралы ақпарат оқиға болғаннан кейін бірден Басқару серверіне жеткізіледі.

Басқару сервері қашықта орналасса, яғни ұйымның желісінен тыс болса, клиент құрылғылар оған интернет арқылы қосылады.

Құрылғыларды интернет арқылы Басқару серверіне қосу үшін келесі шарттар орындалуы керек:

- Қашықтағы Басқару серверінде сыртқы IP мекенжайы болуы және онда 13000 кіріс порты (Желілік агенттерден қосылу үшін) ашық болуы керек. Сондай-ақ, UDP 13000 портын ашу ұсынылады (құрылғыларды өшіру туралы хабарландыруларды қабылдау үшін).

- Құрылғыларда Желілік агенттер орнатылуы керек.

- Желілік агентті құрылғыларға орнатқан кезде қашықтағы Басқару серверінің сыртқы IP мекенжайы көрсетілуі керек. Орнату үшін орнату пакеті пайдаланылса, сыртқы IP мекенжайын **Параметрлер** бөліміндегі орнату пакетінің сипаттарында қолмен көрсету қажет.

- Құрылғыға арналған қолданбалар мен тапсырмаларды басқару мақсатында қашықтағы басқару серверін пайдалану үшін құрылғының сипаттар терезесіндегі **Жалпы** бөліміндегі **Басқару серверімен байланысты үзбеу** ұяшығын таңдаңыз. Жалаушаны қойғаннан кейін, Басқару серверінің қашықтағы құрылғымен синхрондалуын күту керек. Басқару серверімен үздіксіз байланыс бір уақытта 300-ден аспайтын клиент құрылғысын қолдай алады.

Қашықтағы Басқару серверінен келетін тапсырмалардың орындалуын жеделдету үшін құрылғыда 15000 портын ашуға болады. Бұл жағдайда, тапсырманы іске қосу үшін Басқару сервері құрылғымен синхрондалуды күтпей, 15000 порты бойынша Желілік агентке арнайы пакет жібереді.

Kaspersky Security Center бағдарламасы клиент құрылғысының Басқару серверіне қосылымын, операциялардың орындалуы аяқталғаннан кейін қосылым үзілмейтіндей етіп орнатуға мүмкіндік береді. Егер бағдарламалардың күйін үнемі бақылау қажет болса, ал Басқару сервері клиент құрылғысына қосылуды бастау алмаса (мысалы, қосылым желілік экранмен қорғалған, клиент құрылғысында порттарды ашуға тыйым салынған, клиент құрылғысының IP мекенжайы белгісіз) үздіксіз қосылым қажет. Клиент құрылғысы мен Басқару сервері арасындағы үздіксіз қосылымды, құрылғының сипаттар терезесінде, **Жалпы** бөлімінде орнатуға болады.

Ең маңызды құрылғылармен үздіксіз байланыс орнату ұсынылады. Бір уақытта Басқару сервері қолдайтын қосылымдардың жалпы саны шектеулі (300-ге дейін).

Қолмен синхрондау кезінде, қосылым Басқару серверін бастайтын қосылудың көмекші тәсілі қолданылады. Клиент құрылғысына қосылмас бұрын, UDP портын ашу қажет. Басқару сервері клиент құрылғысының UDP портына қосылуға сұрау жібереді. Оған жауап ретінде Басқару сервері сертификаты тексеріледі. Егер Сервер сертификаты клиент құрылғысындағы сертификаттың көшірмесіне сәйкес келсе, қосылым орнатылады.

Синхрондау процесін қолмен іске қосу, бағдарламалардың күйі, тапсырмалардың орындалуы және бағдарламалардың жұмыс статистикасы туралы ағымдағы ақпаратты алу үшін де қолданылады.

Клиент құрылғысын Басқару серверіне қолмен қосу. klmover утилитасы

Егер сізге клиент құрылғысын Басқару серверіне қолмен қосу қажет болса, сіз клиент құрылғысындағы klmover утилитасын пайдалана аласыз.

Желілік агент клиент құрылғысына орнатылған кезде, утилита автоматты түрде Желілік агент орнату қалтасына көшіріледі.

Клиент құрылғысын Басқару серверіне klmover утилитасы арқылы қолмен қосу үшін:

құрылғыда klmover утилитасын пәрмен жолынан іске қосыңыз.

Пәрмен жолынан іске қосылған кезде klmover утилитасы қолданылатын кілттерге байланысты келесі әрекеттерді орындайды:

- Желілік агент көрсетілген параметрлермен Басқару серверіне қосылады;
- операцияның нәтижелерін оқиғалар журналының файлына жазып алады немесе оларды экранға шығарады.

Қосылым шлюздері арқылы басқару серверіне қосылған клиент құрылғылары үшін klmover утилитасын пайдалана алмайсыз. Мұндай құрылғылар үшін Желілік агентті қайта конфигурациялау немесе желілік агентті қайта орнату және қосылым шлюзін көрсету керек.

Утилитаның пәрмен жолының синтаксисі:

```
klmover [-logfile <file name>] [-address <сервер мекенжайы>] [-pn <порт нөмірі>] [-ps <SSL порт нөмірі>] [-nossl] [-cert <сертификат файлының жолы>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Утилитаны іске қосу үшін әкімші құқықтары қажет.

Кілттердің сипаттамалары:

- `-logfile <файл атауы>` — журнал файлына арналған утилитаны іске қосу нәтижелерін жазыңыз.

  Әдепкі бойынша, ақпарат стандартты шығару ағынында (stdout) сақталады. Егер кілт қолданылмаса, нәтижелер мен қате туралы хабарлар экранға шығады.

- `-address <сервер мекенжайы>` — қосылуға арналған басқару серверінің мекенжайы.

  Мекенжай ретінде құрылғының IP мекенжайын, NetBIOS- немесе DNS атауын көрсетуге болады.

- `-pn <порт нөмірі>` — басқару серверіне шифрланбаған қосылым орнатылатын порт нөмірі.

  Әдепкі бойынша 14000-порт орнатылған.

- `-ps <SSL порты нөмірі>` — басқару серверіне SSL көмегімен шифрланған қосылым орнатылатын SSL портының нөмірі.

  Әдепкі бойынша 13000-порт орнатылған.

- `-nossl` – Басқару серверіне шифрланбаған қосылымды пайдалану.

  Егер кілт пайдаланылмаса, Желілік агент Серверге қорғалған SSL протоколы арқылы қосылады.

- `-cert <сертификат файлына апаратын жол>` — басқару серверіне кіруді аутентификациялау үшін берілген сертификат файлын пайдаланыңыз.

  Егер кілт қолданылмаса, Желілік агент Басқару серверіне алғаш рет қосылған кезде сертификат алады.

- `-silent` – утилитаны интерактивті емес режимде іске қосу.

  Кілтті пайдалану пайдалы болуы мүмкін, мысалы, пайдаланушыны тіркеу кезінде кіру сценарийінен утилитаны іске қосу кезінде.

- `-dupfix` – кілт Желілік агентті орнату дистрибуцияны қолдана отырып, дәстүрлі емес түрде орындалған жағдайда қолданылады, мысалы, диск кескінінен қалпына келтіру арқылы.

- `-virtserv` – виртуалды Басқару серверінің атауы.

- `-cloningmode` – Желілік агенттің дискісін клондау режимі.

  Дискіні клондау режимін конфигурациялау үшін келесі параметрлердің бірін пайдаланыңыз:

  - `-cloningmode` – дискіні клондау режимінің күйін сұрау.
  - `-cloningmode 1` – дискіні клондау режимін қосу.
  - `-cloningmode 0` – дискіні клондау режимін өшіру.

- `-nauninstpwd <құпиясөз>` — кілт желілік агентті жою құпиясөзін көрсету үшін қолданылады.

  Кілт міндетті емес.

Мысалы, Желілік агентті Басқару серверіне қосу үшін келесі пәрменді орындаңыз:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Клиент құрылғысы мен Басқару сервері арасындағы қосылымды туннельдеу

Kaspersky Security Center бағдарламасы Басқару консолінен TCP қосылымдарын Басқару сервері арқылы және одан әрі Желілік агент арқылы басқарылатын құрылғыдағы белгіленген портқа туннельдеуге мүмкіндік береді. Туннельдеу, егер Басқару консолі бар құрылғыны құрылғыға тікелей қосу мүмкін болмаса, Басқару консолі орнатылған құрылғыдағы клиент қолданбасын басқарылатын құрылғыдағы TCP портына қосу үшін қолданылады.

Атап айтқанда, туннельдеу қашықтағы жұмыс үстеліне қосылу үшін қолданылады: бұрыннан бар сессияға қосылу үшін де, жаңа қашықтағы сессияны құру үшін де.

Сондай-ақ, туннельдеуді сыртқы құралдар механизмі арқылы пайдалануға да болады. Атап айтқанда, әкімші осылайша putty утилитасын, VNC клиентін және басқа құралдарды іске қоса алады.

Қашықтағы клиент құрылғысы мен Басқару сервері арасындағы байланысты туннельдеу, құрылғыда Басқару серверіне қосылуға арналған порт қолжетімді болмаған кезде қажет. Құрылғыдағы порт келесі жағдайларда қолжетімді болмауы мүмкін:

- Қашықтағы құрылғы NAT механизмі қолданылатын жергілікті желіге қосылған.
- Қашықтағы құрылғы Басқару серверінің жергілікті желісіне кіреді, бірақ оның порты желілік экранмен жабылған.

Клиент құрылғысының Басқару серверіне қосылуын туннельдеу үшін:

1. Консоль ағашында клиент құрылғысы кіретін топ қалтасын таңдаңыз.
2. **Құрылғылар** қойыншасында құрылғыны таңдаңыз.
3. Құрылғының мәнмәтіндік мәзірінен **Барлық тапсырмалар → Байланысты туннельдеу** тармағын таңдаңыз.
4. Ашылған **Байланысты туннельдеу** терезесінде туннель жасаңыз.

Клиент құрылғысының жұмыс үстеліне қашықтан қосылу

Әкімші құрылғыда орнатылған Желілік агент арқылы клиент құрылғысының жұмыс үстеліне қашықтан қатынаса алады.

Желілік агентті пайдаланып клиент құрылғысына қашықтан қосылу, клиент құрылғысының TCP және UDP порттары қатынасу үшін жабық болған жағдайда да мүмкін болады. Құрылғыға қосылғаннан кейін, әкімші осы құрылғыдағы ақпаратқа толық қатынас алады және онда орнатылған бағдарламаларды басқара алады.

Бұл бөлімде Windows операциялық жүйесі бар клиент құрылғысына және macOS операциялық жүйесі бар клиент құрылғысына Желілік агент арқылы қалай қосылу керектігі сипатталған.

Windows операциялық жүйесі орнатылған клиент құрылғыларына қосылу

Windows операциялық жүйесі бар клиент құрылғысына екі жолмен қашықтан қосылуға болады:

- Microsoft Windows "Қашықтағы жұмыс үстеліне қосылу" стандартты құрамдасының көмегімен.

  Қашықтағы жұмыс үстеліне қосылу Windows mstsc.exe штаттық утилитасы арқылы, осы утилитаның жұмыс параметрлеріне сай орындалады.

- Windows Жұмыс үстелін бірлесіп пайдалану технологиясы көмегімен.

Қашықтағы жұмыс үстеліне қосылу арқылы Windows операциялық жүйесінің көмегімен клиент құрылғысына қосылу

Пайдаланушының қашықтағы жұмыс үстелінің қолданыстағы сеансына қосылу, пайдаланушыны хабарландырусыз жүзеге асырылады. Әкімшіні сеансқа қосқаннан кейін, құрылғының пайдаланушысы сеанстан алдын ала хабарландырусыз өшіріледі.

"Қашықтағы жұмыс үстеліне қосылу" құрамдасы арқылы клиент құрылғысының жұмыс үстеліне қосылу үшін:

1. Басқару консолі ағашына қатынасқыңыз келетін құрылғыны таңдаңыз.
2. Құрылғының мәнмәтіндік мәзірінен **Барлық тапсырмалар → Құрылғыға қосылу → Жаңа RDP сеансы** тармағын таңдаңыз.

   Нәтижесінде, қашықтағы жұмыс үстеліне қосылу үшін Windows ОЖ-нің mstsc.exe стандартты утилитасы іске қосылады.
3. Утилитаның ашылатын терезелеріндегі нұсқауларды орындаңыз.

Клиент құрылғысына қосылғаннан кейін, клиент құрылғысының жұмыс үстелі Microsoft Windows қашықтан қосылу терезесінде қолжетімді.

Windows жұмыс үстелін бірлесіп пайдалану арқылы Windows операциялық жүйесінің көмегімен клиенттік құрылғыға қосылу

Қолданыстағы қашықтағы жұмыс үстелі сеансына қосылған кезде, құрылғыдағы осы сеанстың пайдаланушысы әкімшіден қосылуға сұрау алады. Құрылғымен қашықтан жұмыс істеу процесі және осы жұмыстың нәтижелері туралы ақпарат Kaspersky Security Center есептерінде сақталмайды.

Әкімші клиент құрылғысында қолданылатын сеансқа, сол сеанста жұмыс істейтін пайдаланушыны ажыратпай, қосыла алады. Бұл жағдайда, құрылғыдағы әкімші мен сеанс пайдаланушысы жұмыс үстеліне ортақ қол жеткізе алады.

Әкімші қашықтағы клиент құрылғысында әрекеттер аудитін конфигурациялай алады. Аудит барысында, бағдарлама әкімші ашқан және/немесе өзгерткен клиент құрылғысындағы файлдар туралы ақпаратты сақтайды.

Windows жұмыс үстелін бірлесіп пайдалану арқылы клиент құрылғысының жұмыс үстеліне қосылу үшін келесі шарттар орындалуы керек:

- Әкімшінің жұмыс станциясында Microsoft Windows Vista операциялық жүйесі немесе одан кейінгі нұсқасы орнатылған. Басқару сервері орнатылған құрылғының операциялық жүйесінің түрі Windows компьютерлік бөлісу қызметі арқылы қосылуға шектеу емес.

  Windows нұсқаңызда Windows Жұмыс үстелін бірлесіп пайдалану функциясы қосылғанын тексеру үшін Windows тізімдемесінде CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} қосулы екеніне көз жеткізіңіз.

- Клиент құрылғысында Microsoft Windows Vista операциялық жүйесі немесе одан кейінгі нұсқасы орнатылған.

- Kaspersky Security Center бағдарламасы Осалдықтар мен патчтарды басқаруға арналған лицензияны қолданады.

Windows жұмыс үстелін бірлесіп пайдалану арқылы клиент құрылғысының Windows жұмыс үстеліне қосылу үшін:

1. Басқару консолі ағашына қатынасқыңыз келетін құрылғыны таңдаңыз.

2. Құрылғының мәнмәтіндік мәзірінен **Барлық тапсырмалар** → **Құрылғыға қосылу** → **Windows компьютерлік бөлісу қызметін пайдалану** тармағын таңдаңыз.

3. **Қашықтағы жұмыс үстелінің сеансын таңдау** ашылған терезесінде, қосылу қажеті клиент құрылғысындағы сеансты таңдаңыз.

   Клиент құрылғысына сәтті қосылған жағдайда, бұл құрылғының жұмыс үстелі **Kaspersky қашықтағы жұмыс үстелі сеансын көру құралы** терезесінде қолжетімді болады.

4. Құрылғымен өзара іс-қимылды бастау үшін, **Kaspersky қашықтағы жұмыс үстелі сеансын көру құралы** терезесінің бас терезесінде **Әрекеттер** → **Интерактивті режим** тармағын таңдаңыз.

Kaspersky қашықтағы жұмыс үстелі сеансын көру құралы утилитасы жұмыс істеуі үшін, коммерциялық лицензия қажет.

macOS операциялық жүйесі орнатылған клиент құрылғыларына қосылу

Әкімші macOS операциялық жүйесі бар құрылғыларға қосылу үшін Virtual Network Computing (VNC) жүйесін қолдана алады.

Қашықтағы жұмыс үстеліне қосылу Басқару сервері құрылғысында орнатылған VNC клиенті арқылы жүзеге асырылады. VNC клиенті пернетақта мен тінтуірдің көмегімен басқаруды клиент құрылғысынан әкімшіге ауыстырады.

Әкімші қашықтағы жұмыс үстеліне қосылған кезде, пайдаланушы әкімшіден хабарландырулар немесе қосылу сұрауларын алмайды. Әкімші клиент құрылғысында қолданылатын сеансқа, сол сеанста жұмыс істейтін пайдаланушыны ажыратпай, қосылады.

VNC клиентін пайдаланып macOS операциялық жүйесі бар клиент құрылғысының жұмыс үстеліне қосылу үшін келесі шарттар орындалуы керек:

- VNC клиенті Басқару сервері құрылғысында орнатылған.
- Клиент құрылғысында қашықтан кіруге және қашықтан басқаруға рұқсат етіледі.
- Пайдаланушы әкімшіге клиент құрылғысына macOS операциялық жүйесіндегі **Айырбастау** параметрлеріне қатынасуға рұқсат берді.

Virtual Network Computing жүйесі арқылы клиент құрылғысының жұмыс үстеліне қосылу үшін:

1. Басқару консолі ағашына қатынасқыңыз келетін құрылғыны таңдаңыз.
2. Құрылғының мәнмәтіндік мәзірінен **Барлық тапсырмалар** → **Байланысты туннельдеу** тармағын таңдаңыз.
3. Ашылған **Байланысты туннельдеу** терезесінде келесі әрекеттердің бірін орындаңыз:
   a. **1. Желілік порт** бөлімінде қосылғыңыз келетін құрылғының желілік порт нөмірін көрсетіңіз.
   Әдепкі бойынша порт нөмірі – 5900.
   b. **2. Туннельдеу** бөлімінде **Туннель жасау** түймесін басыңыз.
   c. **3. Желілік атрибуттар** бөлімінде **Көшіру** түймесін басыңыз.
4. VNC клиентін ашып, көшірілген желілік атрибуттарды мәтін өрісіне қойыңыз. **Enter** пернесін басыңыз.
5. Пайда болған терезеде сертификат параметрлерін қарап шығыңыз. Егер сіз сертификатты пайдалануға келіссеңіз, **Иә** түймесін басыңыз.
6. **Түпнұсқалық растама** терезесінде клиент құрылғысының есептік деректерін көрсетіп, **OK** түймесін басыңыз.

Windows компьютерлік бөлісу қызметі арқылы құрылғыларға қосылу

Windows Жұмыс үстелін бірлесіп пайдалану арқылы құрылғыға қосылу үшін:

1. Консоль ағашының **Құрылғылар** қойыншасында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
   Қалтаның жұмыс аймағында құрылғылар тізімі көрсетіледі.
2. Қосылғыңыз келетін құрылғының контекстік мәзірінде **Құрылғыға қосылу** → **Windows компьютерлік бөлісу қызметін пайдалану** тармағын таңдаңыз.
   Қашықтағы жұмыс үстелінің сеансын таңдау терезесі ашылады.

3. **Қашықтағы жұмыс үстелінің сеансын таңдау** терезесінде құрылғыға қосылу үшін пайдаланылатын жұмыс үстелі сессиясын таңдаңыз.

4. **OK** түймесін басыңыз.

Құрылғыға қосылу орындалады.

Клиент құрылғысын қайта іске қосуды конфигурациялау

Kaspersky Security Center жұмыс істеп тұрған, орнатылған немесе жойылған кезде клиент құрылғысын қайта іске қосу қажет болуы мүмкін. Қайта іске қосу параметрлерін тек Windows басқаруымен жұмыс істейтін құрылғылар үшін конфигурациялауға болады.

Клиент құрылғысын қайта іске қосуды конфигурациялау үшін:

1. Консоль ағашында қайта іске қосуды конфигурациялау үшін басқару тобын таңдаңыз.

2. Топтың жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.

3. Саясаттар тізімінен Kaspersky Security Center Желілік агенті саясатын таңдап, саясаттың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

4. Саясат сипаттары терезесінде **Өшіріп қайта қосуды басқару** бөлімін таңдаңыз.

5. Құрылғыны қайта іске қосу қажет болса, орындалатын әрекетті таңдаңыз:

   - Автоматты түрде қайта іске қосуды болдырмау үшін **Операциялық жүйені қайта жүктемеу** таңдаңыз.

   - Автоматты түрде қайта іске қосуға рұқсат беру үшін **Қажет болса, операциялық жүйені автоматты түрде қайта іске қосыңыз** тармағын таңдаңыз.

   - Пайдаланушыда қайта іске қосу сұрауын қосу үшін **Пайдаланушыдан әрекетті орындауды сұрау** тармағын таңдаңыз.

   Сіз қайта іске қосу сұрауының жиілігін көрсете аласыз, тиісті жалаушалар мен аралықтарды белгілеу арқылы құрылғыдағы бұғатталған сессияларда бағдарламаларды мәжбүрлеп қайта іске қосуды және мәжбүрлеп жабуды қоса аласыз.

6. Өзгерістерді сақтау және саясат сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

Нәтижесінде, құрылғының операциялық жүйесін қайта іске қосу конфигурацияланады.

Қашықтағы клиент құрылғысындағы әрекеттер аудиті

Бағдарлама Windows жүйесінде жұмыс істейтін қашықтағы клиент құрылғыларында әкімші әрекеттеріне аудит жүргізуге мүмкіндік береді. Аудит барысында, бағдарлама әкімші ашқан және/немесе өзгерткен құрылғыдағы файлдар туралы ақпаратты сақтайды. Әкімші әрекеттерінің аудиті келесі шарттар орындалған кезде қолжетімді:

- Осалдықтар мен патчтарды басқаруға арналған лицензия әлдеқашан қолданылады;

- әкімшінің қашықтағы құрылғының жұмыс үстелін бірлесіп пайдалануға құқығы бар.

Қашықтағы клиент құрылғысында әрекеттер аудитін қосу үшін:

1. Консоль ағашында әкімші әрекетінің аудитін конфигурациялау үшін басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын таңдаңыз.
3. Kaspersky Security Center Желілік агенті саясатын таңдап, саясаттың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
4. Саясат сипаттары терезесінде **Windows компьютерлік бөлісу қызметін пайдалану** бөлімін таңдаңыз.
5. **Аудитті қосу** жалаушасын қойыңыз.
6. **Оқу кезінде бақыланатын файлдардың маскалары** және **Өзгерткен кезде бақыланатын файлдардың маскалары** тізіміндеріне аудит кезінде бағдарлама әрекеттерді бақылайтын файл бүркеніштерін қосыңыз.

   Әдепкі бойынша, бағдарлама .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt және .pdf кеңейтімдері бар файлдармен жасалатын әрекеттерді қадағалайды.
7. Өзгерістерді сақтау және саясат сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

Нәтижесінде, жұмыс үстеліне ортақ қатынасу кезінде қашықтағы пайдаланушы құрылғысындағы әкімші әрекеттерінің аудиті конфигурацияланады.

Қашықтағы құрылғыдағы әкімші әрекеттері туралы жазбалар мында сақталады:

- қашықтағы құрылғыдағы оқиғалар журналында;
- қашықтағы құрылғыдағы Желілік агент қалтасында орналасқан syslog кеңейтімі бар файлда (мысалы, C:\ProgramData\KasperskyLab\adminkit\1103\logs);
- Kaspersky Security Center оқиғалар дерекқорында.

Клиент құрылғысы мен Басқару сервері арасындағы қосылымды тексеру

Kaspersky Security Center бағдарламасы, клиент құрылғысы мен Басқару серверінің арасындағы қосылымды автоматты түрде немесе қолмен тексеруге мүмкіндік береді.

Қосылымды автоматты түрде тексеру Басқару серверінде орындалады. Қосылымды қолмен тексеру құрылғыда жүзеге асырылады.

Клиент құрылғысы мен Басқару серверінің арасындағы қосылымды автоматты түрде тексеру

Басқару сервері мен клиент құрылғысы арасындағы қосылымды автоматты түрде тексеруді іске қосу үшін:

1. Консоль ағашында құрылғы кіретін басқару тобын таңдаңыз.
2. Басқару тобының жұмыс аймағында, **Құрылғылар** қойыншасында құрылғыны таңдаңыз.
3. Құрылғының мәнмәтіндік мәзірінен **Құрылғының қолжетімділігін тексеру** тармағын таңдаңыз.

Нәтижесінде, құрылғының қолжетімділігі туралы ақпарат бар терезе ашылады.

Клиент құрылғысы мен Басқару серверінің арасындағы қосылымды қолмен тексеру. klnagchk утилитасы

Сіз klnagchk утилитасы арқылы қосылымды тексеріп, клиент құрылғысының Басқару серверіне қосылу параметрлері туралы толық ақпарат ала аласыз. klnagchk утилитасы Желілік агентті орнату қалтасында орналасқан.

Пәрмен жолынан іске қосылған кезде klnagchk утилитасы қолданылатын кілттерге байланысты келесі әрекеттерді орындайды:

- Құрылғыда орнатылған Желілік агентті Басқару серверіне қосу параметрлерінің мәндерін экранға шығарады немесе оқиғалар журналының файлына енгізеді.
- Желілік агенттің статистикасын (соңғы іске қосылған сәттен бастап) және утилитаның нәтижелерін оқиғалар журналының файлына жазады немесе ақпаратты экранға шығарады.
- Желілік агент пен Басқару сервері арасындағы байланысты орнатуға тырысады.

  Егер байланыс орнатылмаса, утилита Басқару сервері орнатылған құрылғының күйін тексеру үшін ICMP пакетін жібереді.

klnagchk утилитасын пайдалану арқылы клиент құрылғысы мен Басқару сервері арасындағы байланысты тексеру үшін,

Желілік агент орнатылған құрылғыда жергілікті әкімшілердің есептік жазбасы астындағы пәрмен желісінен klnagchk утилитасын іске қосыңыз.

Утилитаның пәрмен жолының синтаксисі:

```
klnagchk [-logfile <файл атауы>] [-sp] [-savecert <сертификат файлына апаратын жол>]
[-restart][-sendhb]
```

Кілттердің сипаттамалары:

- `-logfile <файл атауы>` – Желілік агентті Серверге қосу параметрлерінің мәндерін және утилитаның нәтижелерін журнал файлына жазып алады.

  Әдепкі бойынша, ақпарат стандартты шығару ағынында (stdout) сақталады. Егер кілт қолданылмаса, параметрлер, нәтижелер мен қате туралы хабарлар экранға шығады.

- `-sp` – прокси-сервердегі пайдаланушының түпнұсқалық растамасы үшін құпиясөзді көрсетеді.

  Басқару серверіне қосылу прокси-сервер арқылы жүзеге асырылса, кілт қолданылады.

- `-savecert <файл атауы>` – көрсетілген файлдағы Басқару серверіне қатынасудың түпнұсқалық растамасы үшін сертификатты сақтайды.
- `-restart` – утилита аяқталғаннан кейін Желілік агентті іске қосады.
- `-sendhb` – Желілік агентті Басқару серверімен синхрондауды іске қосады.

Іске қосылғаннан кейін, klnagchk утилитасы Желілік агент конфигурация файлдарына қатынасады және қосылым параметрлерін көрсетеді. Бұл параметрлер Желілік агентті орнату кезінде және Желілік агент саясаты параметрлерінде белгіленеді:

- `Current device` – Windows желісіндегі клиент құрылғысының атауы.
- `Network Agent version` – құрылғыда орнатылған Желілік агент нұсқасының нөмірі (патчтарымен).
- `Administration Server address` – Басқару серверінің мекенжайы.
- `Use SSL` – Басқару серверіне қосылу кезінде қорғалған қосылымның пайдаланылатынын көрсететін параметр.

  Ықтимал мәндер:

  - 0 – қорғалған арна пайдаланылмайды.
  - 1 – қорғалған арна пайдаланылады.
- `Compress traffic` – клиент құрылғысы мен Басқару сервері арасындағы трафиктің қысылады ма екенін көрсететін параметр.
- `Numbers of the Administration Server SSL ports` – қорғалған арнаны пайдалану кезінде Басқару серверіне қосылуға рұқсат етілген порттардың нөмірлері.
- `Numbers of the Administration Server ports` – әдеттегі қосылымды пайдаланған кезде Басқару серверіне қосылуға рұқсат етілген порттар саны.
- `Use proxy server` – прокси-сервердің пайдаланылатынын көрсететін параметр.

  Ықтимал мәндер:

  - 0 – прокси-сервер пайдаланылмайды.
  - 1 – прокси-сервер қолданылуда.
- `Address` – қос нүктемен бөлінген прокси-сервердің мекенжайы мен порты. Бұл параметр прокси-серверді пайдалансаңыз ғана пайда болады.
- `User name` – прокси-серверге кіруге арналған пайдаланушы аты. Бұл параметр прокси-серверді пайдалансаңыз ғана пайда болады.
- `Password` – прокси-серверге кіруге арналған құпиясөз. Бұл параметр прокси-серверді пайдалансаңыз ғана пайда болады. Прокси-сервер құпиясөзін көрсету үшін пәрмендегі `sp` қосқышын пайдалану керек.
- `Administration Server certificate` – клиент құрылғысында Басқару сервер сертификаты бар-жоғын көрсететін параметр. Мысалы, Желілік агент Басқару серверіне ешқашан қосылмаған болса, сертификат болмауы мүмкін.

  Ықтимал мәндер:

  - `not installed` – клиент құрылғысында Басқару сервері сертификаты жоқ.
  - `available` – клиент құрылғысында Басқару сервері сертификаты бар.
- `Open UDP port` – Басқару серверінен синхрондау сұрауларын алу үшін Желілік агент UDP портын пайдаланады ма екенін көрсететін параметр.

Ықтимал мәндер:

- 0 – Басқару серверінен синхрондау сұрауларын алу үшін UDP порты жабық.
- 1 – Басқару серверінен синхрондау сұрауларын қабылдау үшін UDP порты ашық.

- `Numbers of UDP ports` – Желілік агент пайдалана алатын UDP порттарының нөмірлері.
- `Location name` – құрылғының желідегі орны.
- `State of network location` – клиент құрылғысын бір Басқару серверінің қосылым профилінен екіншісіне ауыстыруға болады ма екенін көрсететін параметр.

  Ықтимал мәндер:

  - `Enabled` – байланыс профилін Басқару серверіне клиент құрылғысы үшін ауыстырып қосуға болады.
  - `Disabled` – байланыс профилін Басқару серверіне клиент құрылғысы үшін ауыстырып қосу мүмкін емес.

- `Profile to use` – Басқару серверіне байланыс профилі.
- `Condition` – клиент құрылғысы қосылған желінің IP мекенжайы және ішкі желі маскасы.
- `Synchronization interval (min)` – стандартты синхрондау аралығы.
- `Connection timeout (in seconds)` – қосылымды күту уақыты.
- `Send / receive timeout (in seconds)` – оқу-жазу операциялары үшін қосылымды күту уақыты.
- `Device ID` – желідегі құрылғы идентификаторы. `Device ID` белгіленген Басқару сервері басқаратын клиент құрылғылары үшін бірегей болып табылады.
- `Locations of connection gateways` – қосылым шлюзі арқылы клиент құрылғысын Басқару серверіне қосуға арналған параметрлер.
- `Location of distribution points` – тарату нүктесінің көмегімен клиент құрылғысын Басқару серверіне қосуға арналған параметрлер.
- `Connection with server` – қосылым шлюзінің Басқару серверімен тұрақты байланысы бар-жоғын көрсететін параметр. Параметр клиент құрылғысы қосылу шлюзі рөлінде әрекет ететін жағдайда ғана көрсетіледі.

  Ықтимал мәндер:

  - `active` – қосылым шлюзінің Басқару серверімен тұрақты қосылымы бар.
  - `inactive` – қосылым шлюзінің Басқару серверімен тұрақты қосылымы жоқ.

- `Connection with server through connection gateway` – қосылу шлюзі арқылы Басқару серверіне қосылымның дұрыс орнатылғанын көрсететін параметр. Параметр клиент құрылғысы қосылу шлюзі рөлінде әрекет ететін жағдайда ғана көрсетіледі.

Ықтимал мәндер:

- `active` – қосылу шлюзі арқылы Басқару серверімен қосылым дұрыс орнатылды.
- `inactive` – қосылу шлюзі арқылы Басқару серверімен қосылым дұрыс орнатылмаған.

Сондай-ақ, klnagchk утилитасының шығысында келесі жолақтардың бірі болуы мүмкін:

- `Administration Server is installed on this device` – klnagchk утилитасы Басқару сервері құрылғысында іске қосылған.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – klnagchk утилитасы қосылым шлюзі режимінде желілік агент орнатылған құрылғыда іске қосылған. Конфигурацияланған қосылу шлюзі Басқару серверінен қосылымды күтеді, бірақ Басқару сервері құрылғыны басқарылатын құрылғылар арасында тізімдемейді. Басқару сервері қосылу шлюзіне қосылуды бастағанына көз жеткізуіңіз керек.
- `This device is a connection gateway` – klnagchk утилитасы қосылу шлюзі рөлін атқаратын құрылғыда іске қосылады.
- `Acts as a distribution point` – klnagchk утилитасы тарату нүктесі рөлін атқаратын құрылғыда іске қосылады.

klnagchk утилитасы Желілік агент қызметінің күйін тексереді. Қызмет іске қосылмаса, утилита тоқтайды. Егер қызмет іске қосылған болса, утилита келесі қосылымдар статистикасын көрсетеді:

- `Total number of synchronization requests` – клиент құрылғысын Басқару серверіне қосу әрекеттерінің саны.
- `The number of successful synchronization request` – клиент құрылғысын Басқару серверіне қосудың сәтті әрекеттерінің саны.
- `Total number of synchronizations` – клиент құрылғысы параметрлерін Басқару сервері параметрлерімен синхрондау әрекеттерінің саны.
- `The number of successful synchronizations` – клиент құрылғысының параметрлерін Басқару серверімен синхрондаудың сәтті әрекеттерінің саны.
- `Date/time of the last request for synchronization` – соңғы қосылымның күні мен уақыты.

Басқару сервері мен Желілік агент арасындағы қосылымды талданған кезде `Total number of synchronization requests` және `The number of successful synchronization request` пайдалану керек. Клиент құрылғысының параметрлері Басқару серверінің параметрлері өзгертілген жағдайда ғана (мысалы, жаңа тапсырмалар қосылғанда немесе саясат параметрлері өзгертілгенде) Басқару серверінің параметрлерімен синхрондалады. Әйтпесе, `Total number of synchronizations` және `The number of successful synchronizations` параметрлерінің мәндері өзгермейді.

Желілік агентті басқару серверіне қосуға қатысты мәселелерді шешу туралы қосымша ақпарат алу үшін Kaspersky Security Center жиі қойылатын сұрақтарын қараңыз.

Құрылғыны Басқару серверіне қосу уақытын тексеру туралы

Құрылғы өшірілген кезде Желілік агент Басқару серверін өшіру туралы хабарлайды. Басқару консолінде мұндай құрылғы өшірулі болып көрсетіледі. Алайда, Агент барлық жағдайда Басқару серверіне хабарлай алмайды. Сол себепті, Басқару сервері әрбір құрылғы үшін ара-тұра **Басқару серверіне қосылған уақыты** атрибутын талдап тұрады (атрибуттың мәні Басқару консолінде, **Жалпы** бөліміндегі құрылғы сипаттарында көрсетіледі) және оны Желілік агенттің қолданыстағы параметрлерінен синхрондау кезеңімен салыстырады. Құрылғы үш синхрондау кезеңінен артық уақыт бойы байланысқа шықпаса, онда мұндай құрылғы өшірулі болып белгіленеді.

Басқару серверіндегі клиент құрылғыларын сәйкестендіру

Клиент құрылғыларын сәйкестендіру олардың атаулары негізінде жүзеге асырылады. Құрылғы атауы Басқару серверіне қосылған барлық құрылғы атауларының арасында бірегей.

Құрылғының атауы Басқару серверіне Windows желісінде сауалнама жүргізіп, онда жаңа құрылғы табылған кезде немесе құрылғыға орнатылған Желілік агенттің Басқару серверіне алғаш рет қосылған кезде беріледі. Әдепкі бойынша, атау Windows желісіндегі құрылғының атауына сәйкес келеді (NetBIOS атауы). Басқару серверінде осындай атауы бар құрылғы тіркелген болса, онда жаңа құрылғының атына реттік нөмірі бар жалғау қосылады, мысалы: **<Аты>-1**, **<Аты>-2**. Осы атауы бар құрылғы басқару тобының құрамына кіреді.

Құрылғыларды басқару тобының құрамына жылжыту

Бастапқы, сондай-ақ мақсаты басқару топтары үшін (немесе осы топтар тиесілі болып табылатын Басқару сервері үшін) **Басқару топтарын басқару** аймағында **Өзгерту** құқықтары болған кезде ғана құрылғыларды бір басқару тобынан екіншісіне жылжытуға болады.

Бір немесе бірнеше құрылғыны таңдалған басқару тобының құрамына қосу үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын ашыңыз.
2. **Басқарылатын құрылғылар** қалтасында клиент құрылғылары қосылатын топқа сәйкес келетін салынған қалтасын таңдаңыз.

   Егер сіз құрылғыларды **Басқарылатын құрылғылар** тобына қосқыңыз келсе, бұл қадамды өткізіп жіберуге болады.
3. **Құрылғылар** қойыншасындағы таңдалған басқару тобының жұмыс аймағында келесі тәсілдердің бірімен құрылғыларды топқа қосу процесін бастаңыз:

   - Құрылғыларды құрылғылар тізімімен жұмыс істеу блогындағы **Құрылғыларды топқа жылжыту** түймесі арқылы топқа қосыңыз.
   - Құрылғылар тізімінің контекстік мәзірінен **Жасау** → **Құрылғы** тармағын таңдаңыз.

Нәтижесінде, құрылғыларды жылжыту шебері іске қосылады. Оның нұсқауларын орындай отырып, құрылғыларды топқа жылжыту жолын анықтаңыз және топқа кіретін құрылғылардың тізімін жасаңыз.

Құрылғылар тізімін қолмен қалыптастырып жатсаңыз, құрылғының мекенжайы ретінде сіз IP мекенжайын (немесе IP аралығын), NetBIOS немесе DNS атауын пайдалана аласыз. Құрылғылар тізіміне құрылғыны қосқан кезде немесе құрылғыларды табу нәтижесінде Басқару сервері дерекқорына ақпарат қосылған құрылғыларды ғана қолмен жылжытуға болады.

Файлдан құрылғылар тізімін импорттау үшін файлды TXT пішімінде қосылатын құрылғылардың мекенжайларының тізімімен көрсету қажет. Әр мекенжай бөлек жолда орналасуы керек.

Шебер аяқталғаннан кейін, таңдалған құрылғылар басқару тобының құрамына енеді және олар үшін Басқару сервері берген атаулары бар құрылғылар тізімінде көрсетіледі.

Құрылғыны таңдалған басқару тобына тінтуірмен **Тағайындалмаған құрылғылар** қалтасынан басқару тобы қалтасына апару арқылы жылжытуға болады.

Клиент құрылғылары үшін Басқару серверін ауыстыру

Клиент құрылғылары жұмыс істейтін Басқару серверін *Басқару серверін ауыстыру* тапсырмасы арқылы басқа Сервермен ауыстыруға болады.

Клиент құрылғылары жұмыс істейтін Басқару серверін басқа Сервермен ауыстыру үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағындағы **Жаңа тапсырма** түймесі арқылы тапсырманы жасау шеберін іске қосыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Тапсырма түрін таңдау** бетінде **Kaspersky Security Center басқару сервері** түйінін таңдаңыз, **Кеңейтілген** қалтасын жайыңыз, содан кейін **Басқару серверін ауыстыру** тапсырмасын таңдаңыз.
4. Ашылған терезелерде клиент құрылғыларына арналған басқару серверін өзгерту шарттарына келісетініңізді растау үшін **OK** түймесін басыңыз.
5. Шебердің **Параметрлер** қадамында таңдалған құрылғыларды басқару үшін қолданғыңыз келетін басқару серверін таңдаңыз:

   - **Басқа негізгі Басқару серверіне өзгертіңіз**

     Клиент құрылғыларын басқа негізгі басқару серверіне жылжыту үшін келесі басқару серверінің қосылым параметрлерін көрсетіңіз:

     1. **Басқару сервері** өрісінде жаңа негізгі басқару серверінің мекенжайын көрсетіңіз.
     2. **Порт** өрісінде басқару серверіне қосылу үшін порт нөмірін көрсетіңіз.

        Әдепкі бойынша 14000-порт орнатылған.
     3. **SSL порты** өрісінде негізгі басқару серверінің SSL портының нөмірін көрсетіңіз.

        Әдепкі бойынша 13000-порт орнатылған.
     4. Қажет болса, **Прокси-серверді пайдалану** құсбелгісін қойыңыз.

        Бұл құсбелгі тазаланса, құрылғыны басқару серверіне қосу үшін тікелей қосылым қолданылады.

Бұл құсбелгі қойылса, прокси-сервер параметрлерін көрсетіңіз:

- **Прокси-сервердің мекенжайы**
- **Прокси-сервердің порты**

Прокси-серверге аутентификация қажет болса, прокси-сервер қосылымы орнатылатын есептік жазбаның **Пайдаланушы аты** және **Құпиясөз** өрістерінде есептік жазбаның кіру деректерін көрсетіңіз. Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.

5. Қажет болса, жаңа басқару сервері сертификатын жүктеп салыңыз.

- **Осы негізгі сервердегі басқа виртуалды Басқару серверіне өзгертіңіз**

  Клиент құрылғыларын ағымдағы негізгі басқару серверіндегі виртуалды басқару серверіне жылжыту үшін осы опцияны таңдаңыз. Ол үшін **Виртуалды Басқару серверінің атауы** өрісінде қажетті виртуалды басқару серверінің атауын көрсетіңіз.

Қажет болса, желілік агентті қайта іске қоспай тұрып, күту уақытын көрсетіңіз.

6. Шебердің осы қадамында тапсырма тағайындалатын құрылғыларды таңдаңыз:

- **Басқару серверімен анықталған желілік құрылғыларды таңдау**. Құрылғылар жинағына тапсырма тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.
- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**. Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.
- **Құрылғы таңдауына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған таңдауды құрайтын құрылғыларға тағайындалады. Алдын ала анықталған таңдауды немесе өз таңдауыңызды көрсете аласыз.
- **Басқару тобына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады.

7. Шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында есептік жазба параметрлерін көрсетіңіз:

- **Әдепкі есептік жазба**

  Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Есептік жазбаны көрсету**

  Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

  - **Есептік жазба**

    Тапсырманы іске қосатын есептік жазба.

- **Құпиясөз**

  Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

8. Шебердің **Тапсырма кестесін конфигурациялау** қадамында тапсырманы іске қосу кестесін жасауға болады. Қажет болса, келесі параметрлерді конфигурациялаңыз:

   - **Кесте бойынша іске қосу:**

     Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

     - **Күн сайын (жазғы уақытқа өтуге қолдау көрсетілмейді)**

       Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Бұл кесте жазғы уақытты сақтауды қолдамайды. Демек, уақыт жаздың басында немесе соңында бір сағатқа алға немесе артқа ауысқанда, тапсырманың нақты іске қосылу уақыты өзгермейді.

       Бұл кестені пайдалану ұсынылмайды. Бұл, Kaspersky Security Center кері үйлесімділігі үшін қажет.

       Әдепкі бойынша, тапсырма күн сайын, ағымдағы жүйелік уақытта іске қосылады.

     - **Апта күндері бойынша**

       Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

       Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

     - **Ай сайын**

       Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

       Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

       Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

     - **Бір рет**

       Тапсырма көрсетілген күн мен уақытта тек бір рет орындалады (тапсырманың жасалған күніне сәйкес).

     - **Қолмен**

       Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **Дереу**

       Тапсырма құрылғы желіде көрінгеннен кейін немесе құрылғы тапсырма ауқымына қосылғаннан кейін бірден іске қосылады.

   - **Өткізіп алынған тапсырмаларды іске қосу**

     Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

     Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

9. Шебердің осы қадамында жасап жатқан тапсырманың атауын көрсетіңіз.
10. Шебердің жұмысын аяқтау үшін шебердің **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

    Шебердің жұмысы аяқталғаннан кейін тапсырманың бірден іске қосылғанын қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** құсбелгісін қойыңыз.

Тапсырма аяқталғаннан кейін, ол жасалған клиент құрылғылары тапсырма параметрлерінде көрсетілген басқару серверінің басқаруына өтеді.

Басқару сервері шифрлауды және деректерді қорғауды басқаруды қолдаса, онда *Басқару серверін ауыстыру* тапсырмасын жасау кезінде ескерту көрсетіледі. Ескертуде басқа Сервер басқаратын құрылғыларды ауыстырғаннан кейін құрылғыларда шифрланған деректер болған кезде пайдаланушыларға бұрын жұмыс істеген шифрланған деректерге ғана қатынасу мүмкіндігі берілетіні туралы ақпарат бар. Басқа жағдайларда, шифрланған деректерге қатынас берілмейді. Шифрланған деректерге қатынасу ұсынылмайтын скрипттерің толық сипаттамасы Kaspersky Endpoint Security for Windows анықтамасында берілген.

Басқа Басқару серверіне қосылу шлюздері арқылы Басқару серверіне қосылған құрылғыларды жылжыту

Басқа басқару серверіне қосылу шлюздері арқылы басқару серверіне қосылған басқа құрылғыларды жылжыту. Мысалы, басқару серверінің басқа нұсқасын орнату қажет болғанда және артық уақыт алатындықтан, құрылғыларға желілік агентті қайта орнатқыңыз келмесе, осы әрекет қажет болуы мүмкін.

Нұсқауларда сипатталған пәрмендер әкімші құқықтары бар тіркелгі бойынша клиент құрылғыларда орындалуы керек.

Қосылым шлюзі арқылы қосылған құрылғыны басқа Басқару серверге жылжыту үшін:

1. Жаңа басқару серверіне ауысу үшін klmover утилитасын `-address <сервер мекенжайы>` параметрімен іске қосыңыз.
2. `klnagchk -nagwait -tl 4` пәрменді орындаңыз.
3. Жаңа қосылым шлюзін орнату үшін келесі пәрмендерді орындаңыз:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<gateway_ip_or_name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Бұл жердегі `<gateway ip or name>` — интернеттен қолжетімді қосылым шлюзінің мекенжайы.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` – қосылым шлюзі тыңдайтын TCP портының нөмірі.
4. Network AgentЖелілік агент қызметін іске қосу үшін `klnagchk -restart -tl 4` пәрменді орындаңыз.

Құрылғы жаңа и серверіне жылжытылады және жаңа қосылым шлюзі арқылы қосылады.

Кластерлер және серверлердің массивтері

Kaspersky Security Center кластерлік технологияны қолдайды. Желілік агент Басқару серверіне клиент құрылғысында орнатылған бағдарлама сервер массивінің бөлігі екені туралы ақпарат берсе, онда клиент құрылғысы кластер түйініне айналады. Кластер сервер белгішелері ( ) бар Консоль ағашында **Басқарылатын құрылғылар** қалтасындағы бөлек нысан ретінде қосылады.

Кластердің бірнеше типтік сипаттарын бөлектеуге болады:

- Кластер және оның түйіндерінің кез келгені әрдайым бір басқару тобында орналасады.
- Әкімші қандай да бір кластер түйінін басқа жерге көшіргісі келсе, түйін өзінің бастапқы орналасқан жеріне оралады.
- Әкімші кластерді басқа топқа көшіргісі келсе, оның барлық түйіндері де онымен бірге көшірілетін болады.

Клиент құрылғыларын қашықтан қосу, өшіру және қайта іске қосу

Kaspersky Security Center бағдарламасы клиент құрылғыларын қашықтан басқаруға, қосуға, өшіруге және қайта іске қосуға мүмкіндік береді.

Клиент құрылғыларын қашықтан басқару үшін:

1. Құрылғыларды басқаратын Басқару серверіне қосылыңыз.
2. Келесі тәсілдердің бірімен құрылғыларды басқару тапсырмасын жасаңыз:
   - Таңдалған басқару тобына кіретін құрылғыларды қосу, өшіру немесе қайта іске қосу керек болса, таңдалған топ үшін тапсырманы жасаңыз.
   - Әртүрлі басқару топтарына кіретін немесе басқару топтарына кірмейтін құрылғыларды қосу, өшіру немесе қайта іске қосу керек болса, құрылғыларды жинауға арналған тапсырманы жасаңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз. Тапсырманы жасау шеберінің **Тапсырма түрін таңдау** терезесінде **Kaspersky Security Center** торабын таңдап, **Кеңейтілген** қалтасын ашып, **Құрылғыларды басқару** тапсырмасын таңдаңыз.
3. Жасалған тапсырманы іске қосыңыз.

   Тапсырма аяқталғаннан кейін, пәрмен (қосу, өшіру немесе қайта іске қосу) таңдалған құрылғыларда орындалатын болады.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты қосылымды пайдалану туралы

Әдепкі бойынша, Kaspersky Security Center бағдарламасында басқарылатын құрылғылар мен Басқару сервері арасында тұрақты байланыс жоқ. Басқарылатын құрылғылардағы Желілік агенттер мезгіл-мезгіл қосылым орнатып, Басқару серверімен синхрондалады. Осы синхрондау сеанстары арасындағы аралық Желілік агенттің саясатында анықталады және әдепкі бойынша 15 минутты құрайды. Ерте синхрондау (мысалы, саясат қолданбасын мәжбүрлеу үшін) қажет болса, басқару сервері қол қойылған желі пакетін UDP 15000 портындағы желілік агентке жібереді. (Басқару сервері бұл пакетті IPv4 немесе IPv6 желісі арқылы жібере алады.) Белгілі бір себептерге байланысты басқару сервері мен басқарылатын құрылғы арасында UDP арқылы қосу мүмкін болмаса, синхрондау аралығында желілік агент пен басқару серверіндегі келесі күнделікті қосылымда синхрондау орындалады.

Алайда, Желілік агентті Басқару серверіне қоспай-ақ кейбір операцияларды орындау мүмкін емес. Бұл операцияларға жергілікті тапсырмаларды іске қосу және тоқтату, басқарылатын бағдарламаның статистикасын алу және туннель құру кіреді. Бұл операциялар орындалуы үшін, басқарылатын құрылғыдағы **Басқару серверімен байланысты үзбеу** опциясын қосуыңыз керек.

Мәжбүрлеп синхрондау туралы

Kaspersky Security Center бағдарламасы басқарылатын құрылғылар үшін күйді, параметрлерді, тапсырмаларды және саясаттарды автоматты түрде синхрондайтынына қарамастан, кейбір жағдайларда әкімші белгілі бір құрылғы үшін ағымдағы уақытта синхрондау орындалғанын нақты білуі керек.

Басқару консоліндегі басқарылатын құрылғылардың контекстік мәзірінде, мәзірдің **Барлық тапсырмалар** тармағында **Мәжбүрлеп синхрондау** пәрмені бар. Kaspersky Security Center 15.1 бағдарламасы осы пәрменді орындаған кезде, Басқару сервері құрылғыға қосылуға тырысады. Егер бұл әрекет сәтті болса, мәжбүрлеп синхрондау орындалады. Әйтпесе, мәжбүрлеп синхрондау Желілік агент Сервермен байланыс орнатқаннан кейін ғана орындалады.

Байланыс кестесі туралы

Желілік агент саясаты сипаттары терезесінде, **Қосылым мүмкіндігі** бөлімінде, **Байланыс кестесі** салынған бөлімінде Желілік агент деректерді Басқару серверіне беретін уақыт аралықтарын белгілеуге болады.

Қажет болғанда қосылу. Егер бұл нұсқа таңдалса, байланыс Желілік агент деректерді Басқару серверіне жіберуі қажет болған кезде орнатылады.

Көрсетілген кезеңдерде қосылу. Егер бұл нұсқа таңдалса, Желілік агентті Басқару серверіне қосу белгілі бір уақыт аралығында жүзеге асырылады. Бірнеше қосылу кезеңдерін қосуға болады.

Құрылғылардың пайдаланушыларына хабар жіберу

Құрылғылардың пайдаланушыларына хабар жіберу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Келесі тәсілдердің бірімен құрылғылардың пайдаланушыларына хабар жіберу тапсырмасын жасаңыз:
   - Таңдалған басқару тобына кіретін құрылғылардың пайдаланушыларына хабар жіберу керек болса, таңдалған топ үшін тапсырма жасаңыз.
   - Әртүрлі басқару топтарына кіретін немесе ешбір басқару тобына кірмейтін құрылғылардың пайдаланушыларына хабар жіберу керек болса, құрылғыларды жинауға арналған тапсырманы жасаңыз.

Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Тапсырма жасау шебері тапсырмасының түрі терезесінде **Kaspersky Security Center Басқару сервері** торабын таңдап, **Кеңейтілген** қалтасын ашып, **Пайдаланушыға хабар жіберу** тапсырмасын таңдаңыз. Пайдаланушыға тапсырманың көмегімен хабар жіберу тек Windows операциялық жүйесінің басқаруындағы құрылғылар үшін ғана қолжетімді. Сондай-ақ Пайдаланушылардың есептік жазбаларын басқару қалтасының **жұмыс аймағындағы пайдаланушының мәнмәтіндік мәзірінен хабар жібере** аласыз.

4. Жасалған тапсырманы іске қосыңыз.

Тапсырма аяқталғаннан кейін, жасалған хабар таңдалған құрылғылардың пайдаланушыларына жіберілетін болады. Пайдаланушыға тапсырманың көмегімен хабар жіберу тек Windows операциялық жүйесінің басқаруындағы құрылғылар үшін ғана қолжетімді. Сондай-ақ, **Пайдаланушылардың есептік жазбалары** қалтасының жұмыс аймағындағы пайдаланушының мәнмәтіндік мәзірінен хабар жібере аласыз.

Kaspersky Security for Virtualization бағдарламасымен жұмыс істеу

Kaspersky Security Center бағдарламасы виртуалды машиналарды Басқару серверіне қосу мүмкіндігін қолдайды. Виртуалды машиналар Kaspersky Security for Virtualization арқылы қорғалған. Қосымша ақпарат алу үшін осы қолданбаның құжаттамасын қараңыз.

Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Сипаттар терезесін келесі тәсілдердің бірімен ашыңыз:

   - Басқару сервері саясатының мәнмәтіндік мәзіріндегі **Саясаттар** қалтасында **Сипаттар** тармағын таңдаңыз.

   - Басқару тобының мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

2. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Құрылғының күйі** бөлімін таңдаңыз.

3. **Осы кезде Критикалыққа орнату** бөлімінде тізімнен шартқа жалауша қойыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

4. Таңдалған шарт атауын екі рет басып, ашылатын терезеде шарттың қажетті мәнін орнатыңыз.

   Келесі шарттардың мәндерін орнату мүмкін емес: Қауіпсіздік бағдарламасы орнатылмаған, Үйлесімді емес бағдарламалар орнатылды, Бағдарламалық жасақтама осалдықтары анықталды, Ұялы құрылғы параметрлері саясатқа жауап бермейді, Өңделмеген қауіпсіздік мәселелері табылды, Бағдарлама анықтаған құрылғы күйі, Құрылғы басқарылмайтын күйге айналды, Қауіпсіздік бағдарламасы іске қосылмаған, Лицензия мерзімі өтті.

   Қайта іске қосу керек шарты үшін қайта іске қосу себептерін көрсетуге болады. Тізімдегі барлық себептің жанындағы құсбелгі ұяшықтарын таңдауға кеңес береміз.

5. **ОК** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Сипаттар терезесін келесі тәсілдердің бірімен ашыңыз:

   - Басқару сервері саясатының мәнмәтіндік мәзіріндегі **Саясаттар** қалтасында **Сипаттар** тармағын таңдаңыз.

   - Басқару тобының мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

2. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Құрылғының күйі** бөлімін таңдаңыз.

3. **Осы кезде Ескертуге орнату** бөлімінде тізімдегі шарт үшін жалауша қойыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

4. Таңдалған шарт атауын екі рет басып, ашылатын терезеде шарттың қажетті мәнін орнатыңыз.

   Келесі шарттардың мәндерін орнату мүмкін емес: Қауіпсіздік бағдарламасы орнатылмаған, Үйлесімді емес бағдарламалар орнатылды, Бағдарламалық жасақтама осалдықтары анықталды, Ұялы құрылғы параметрлері саясатқа жауап бермейді, Өңделмеген қауіпсіздік мәселелері табылды, Бағдарлама анықтаған құрылғы күйі, Құрылғы басқарылмайтын күйге айналды, Қауіпсіздік бағдарламасы іске қосылмаған, Лицензия мерзімі өтті.

   Қайта іске қосу керек шарты үшін қайта іске қосу себептерін көрсетуге болады. Тізімдегі барлық себептің жанындағы құсбелгі ұяшықтарын таңдауға кеңес береміз.

5. **OK** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Ескерту* күйі тағайындалады.

Құрылғыларға тегтерді тағайындау және тағайындалған тегтерді қарап шығу

Kaspersky Security Center құрылғыларға тегтерді тағайындауға мүмкіндік береді. *Тег* дегеніміз – құрылғыларды топтау, сипаттау, іздеу үшін пайдалануға болатын құрылғы идентификаторы. Құрылғыларға тағайындалған тегтер, құрылғылар іріктемесін жасау, құрылғыларды іздеу және құрылғыларды басқару топтары бойынша бөлу кезінде пайдаланылуы мүмкін.

Тегтерді құрылғыларға қолмен немесе автоматты түрде тағайындауға болады. Құрылғыға тегтерді қолмен тағайындау, құрылғының сипаттарында орындалады және бөлек құрылғыны белгілеу қажет болғанда керек болып қалуы мүмкін. Тегтерді автоматты түрде тағайындау, белгіленген тегтерді тағайындау ережелеріне сәйкес Басқару сервері тарапынан орындалады.

Басқару серверінің сипаттарында, осы Басқару сервері басқаратын құрылғыларға тегтерді автоматты түрде тағайындауды конфигурациялауыңызға болады. Құрылғыларға тегтерді автоматты түрде тағайындау, белгілі бір ережелерді орындау кезінде жүзеге асырылады. Әрбір тегке бөлек ереже сай келеді. Ережелер құрылғының желілік сипаттарына, операциялық жүйеге, құрылғыда орнатылған бағдарламаларға және құрылғының басқа да сипаттарына қатысты қолданылуы мүмкін. Мысалы, Windows операциялық жүйесінің басқаруымен жұмыс істейтін құрылғыларға *Win* тегін тағайындайтын ережені конфигурациялауыңызға болады. Содан соң, Windows операциялық жүйесінің басқаруымен жұмыс істейтін құрылғыларды таңдау және оларға тапсырма тағайындау үшін, осы тегті құрылғы таңдауларын жасау кезінде қолдануға болады.

Сондай-ақ, белгілі бір саясат профильдері белгілі бір тегтерді бір құрылғыларда ғана қолданылуы үшін тегтерді басқарылатын құрылғыда саясат профилін белсендіруге арналған шарт ретінде де қолдана аласыз. Мысалы, *Пайдаланушылар* басқару тобында *Курьер* тегі бар құрылғы пайда болса және *Курьер* тегі бойынша тиісті саясат профилін белсендіру конфигурацияланған болса, онда осы құрылғыға *Пайдаланушылар* тобы үшін жасалған саясаттың өзі емес, оның профилі қолданылады. Саясат профилі осы құрылғыда саясат аясында іске қосуға болмайтын бөлек бағдарламаларды іске қосуға рұқсат бере алады.

Сіз бірнеше тег тағайындау ережесін жасай аласыз. Бірнеше тег тағайындау ережесін жасаған болсаңыз және осы ережелердің шарттары бір уақытты орындалып жатса, бір құрылғыға бірнеше тег тағайындалуы мүмкін. Барлық тағайындалған тегтер тізімін құрылғының сипаттарында қарап шыға аласыз. Әрбір тег тағайындау ережесін қосуға немесе өшіруге болады. Ереже қосулы болса, ол Басқару сервері басқаратын құрылғыларға қатысты қолданылады. Ереже керек болмаса, біраз алдағыда қажет болып қалуы мүмкін болса, оны жоюдың керегі жоқ; **Ережені қосу** жалаушасын алып тастасаңыз жеткілікті. Бұл арада, ереже өшіріліп, **Ережені қосу** жалаушасы қойылмайынша орындалмайды. Ережені жоймай өшіру, бұл ережені тег тағайындау ережелері тізімінен уақытша алып тастап, кейін қайтадан қосу керек болған кезде қажет болып қалуы мүмкін.

Құрылғыларға тегтерді автоматты түрде тағайындау

Басқару сервері сипаттары терезесінде тегтерді автоматты түрде белгілеу ережелерін жасауға және өзгертуге болады.

Құрылғыларға тегтерді автоматты түрде тағайындау үшін:

1. Консоль ағашында тегтерді тағайындау ережелерін белгілеуді қажет ететін Басқару сервері атауы бар түйінді таңдаңыз.

2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесінде **Тегтерді белгілеу ережелері** бөлімін таңдаңыз.

4. **Тегтерді белгілеу ережелері** бөлімінде **Қосылуда** түймесін басыңыз.

   Жаңа ереже терезесі ашылады.

5. **Жаңа ереже** терезесінде ереженің жалпы сипаттарын конфигурациялаңыз:

   - Ереженің атауын көрсетіңіз.

     Ереже атауы 255 таңбадан асуы және арнайы таңбаларды (`"*<>?\:|`) қамтуы мүмкін емес.

   - Ережені **Ережені қосу** жалаушасы көмегімен қосыңыз немесе өшіріңіз.

     Әдепкі бойынша, **Ережені қосу** жалаушасы қойылған.

   - **Тег** өрісінде тег атауын енгізіңіз.

     Тег атауы 255 таңбадан асуы және арнайы таңбаларды (`"*<>?\:|`) қамтуы мүмкін емес.

6. **Шарттар** бөлімінде, жаңа шартты қосу үшін **Қосылуда** түймесін басыңыз немесе қолданыстағы шарттарды өзгерту үшін **Сипаттар** түймесін басыңыз.

   Тегтерді автоматты түрде белгілеу ережесіне арналған шартты жасау шебері терезесі ашылады.

7. **Тегті белгілеу шарты** терезесінде, тег тағайындауға әсер етуі тиісті шарттар үшін жалаушалар қойыңыз. Бірнеше шарт таңдауға болады.

8. Қандай тег тағайындау шарттарын таңдағаныңызға байланысты, шебер тиісті шарттарды конфигурациялау үшін терезелерді көрсетеді. Ереженің іске қосылуын келесі шарттар бойынша конфигурациялаңыз:

   - **Құрылғыны пайдалану немесе белгілі бір желімен байланыстыру** – құрылғының желілік сипаттары (мысалы, Windows желісіндегі құрылғының атауы, құрылғының доменге, IP ауқымына тиесілі болуы).

     Kaspersky Security Center үшін пайдаланып жатқан дерекқорда тіркелімді ескере отырып сұрыптау конфигурацияланған болса, құрылғының DNS атауын көрсеткенде тіркемді ескеріңіз. Әйтпесе, автоматты түрде тег қою ережелері жұмыс істемейді.

   - **Active Directory қызметін пайдалану** – құрылғының Active Directory бөлімшесінде болуы және құрылғының Active Directory тобына мүшелігі.

   - **Анықталған бағдарламалар** – құрылғыда Желілік агенттің болуы, операциялық жүйенің түрі, нұсқасы және архитектурасы.

   - **Виртуалды машиналар** – құрылғының виртуалды машиналардың белгілі бір түріне тиесілі болуы.

   - **Бағдарламалар тізімдемесіндегі бағдарлама орнатылды** – құрылғыда әртүрлі өндірушілердің бағдарламаларының болуы.

9. Шартты конфигурациялағаннан кейін, шарттың атауын енгізіп, шебердің жұмысын аяқтаңыз.

   Қажет болса, бір ереже үшін бірнеше шарт белгілеуге болады. Бұл жағдайда, құрылғылар үшін шарттардың кемінде біреуі орындалса, тег оларға тағайындалады. Қосылған шарттар ереженің сипаттары терезесінде көрсетіледі.

10. **Жаңа ереже** терезесіндегі **ОК** түймесін және Басқару сервері сипаттары терезесіндегі **ОК** түймесін басыңыз.

Жасалған ережелер, таңдалған Басқару сервері басқаратын құрылғыларда орындалады. Құрылғы параметрлері ереженің шарттарына сәйкес келсе, бұл құрылғыға тег тағайындалады.

Құрылғыға тағайындалған тегтерді қарап шығу және конфигурациялау

Құрылғыға тағайындалған барлық тегтердің тізімін қарап шығуға, сондай-ақ құрылғы сипаттары терезесінде тегтерді автоматты түрде тағайындау ережелерін конфигурациялауға өтуге болады.

Құрылғыға тағайындалған тегтерді қарап шығу және конфигурациялау үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын ашыңыз.

2. **Басқарылатын құрылғылар** қалтасының жұмыс аймағында, тағайындалған тегтерін қарап шыққыңыз келетін құрылғыны таңдаңыз.

3. Ұялы құрылғының контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

4. Құрылғы сипаттары терезесінде **Тегтер** бөлімін таңдаңыз.

   Таңдалған құрылғыға тағайындалған тегтер тізімі, сондай-ақ тегті тағайындау тәсілі көрсетіледі: қолмен немесе ереже бойынша.

5. Қажет болса, келесі әрекеттердің бірін орындаңыз:

    - Тег тағайындау ережелерін конфигурациялауға өту үшін **Автоматты түрде тег қою ережелерін орнату** сілтемесі арқылы өтіңіз (Windows операциялық жүйесі бар құрылғылар үшін ғана).
    - Тегті қайта атау үшін, тегті бөлектеп, **Қайта атау** түймесін басыңыз.
    - Тегті жою үшін тегті бөлектеп, **Жою** түймесін басыңыз.
    - Тегті қолмен қосу үшін, тегті **Тегтер** бөлімінің астындағы өріске енгізіп, **Қосу** түймесін басыңыз.

6. **Тегтер** бөлімінде өзгерістер жасаған болсаңыз, өзгерістеріңіз күшіне ену үшін **Қолдану** түймесін басыңыз.
7. **ОК** түймесін басыңыз.

Құрылғының сипаттарында тегті жойсаңыз немесе оның атын өзгертсеңіз, бұл өзгеріс Басқару серверінің қасиеттерінде белгіленген тегтерді тағайындау ережелеріне қолданылмайды. Өзгеріс тек сіз өзгерткен сипаттары бар құрылғыға ғана қолданылады.

Клиент құрылғыларын қашықтан диагностикалау. Kaspersky Security Center қашықтан диагностикалау утилитасы

Kaspersky Security Center қашықтан диагностикалау утилитасы (бұдан әрі – қашықтан диагностикалау утилитасы) клиент құрылғыларында келесі операцияларды қашықтан орындауға арналған:

- Трассалауды қосу және өшіру, трассалау деңгейін өзгерту, трассалау файлын жүктеу.
- Жүйе ақпараты мен қолданба параметрлерін жүктеп алу.
- Оқиғалар журналдарын жүктеу.
- Қолданба үшін дэмп файлын жасау.
- Диагностиканы іске қосу және диагностика нәтижелерін жүктеу.
- Бағдарламаларды іске қосу немесе тоқтату.

Ақауларды жою үшін клиент құрылғысынан жүктелген оқиғалар журналы мен диагностикалық есептерді пайдалануыңызға болады. Сондай-ақ, Kaspersky Техникалық қолдау қызметінің маманы сізден трассалау файлдарын, қоқыс файлдарын, оқиғалар журналын және диагностикалық есептерді Kaspersky талдау мақсатымен клиент құрылғысынан жүктеп алуды сұрауы мүмкін.

Қашықтан диагностикалау утилитасы құрылғыға Басқару консолімен бірге автоматты түрде орнатылады.

Қашықтан диагностикалау утилитасын клиент құрылғысына қосу

Қашықтағы диагностикалау утилитасын клиент құрылғысына қосу үшін:

1. Консоль ағашында кез келген басқару топтарын таңдаңыз.

2. **Құрылғылар** қойыншасында кез келген құрылғының контекстік мәзірінен **Реттелмелі құралдар → Қашықтан диагностикалау** тармағын таңдаңыз.

   Нәтижесінде, қашықтан диагностикалау утилитасының бас терезесі ашылады.

3. Қашықтан диагностикалау утилитасының бас терезесінің бірінші өрісінде құрылғыға қандай құралдармен қосылу керектігін анықтаңыз:

   - **Microsoft Windows желісінің құралдары арқылы қатынасу**.
   - **Басқару серверінің құралдары арқылы қатынасу**.

4. Егер утилитаның негізгі терезесінің бірінші өрісінде сіз **Microsoft Windows желісінің құралдары арқылы қатынасу** нұсқасын таңдасаңыз:

   - **Құрылғы** өрісінде қосылу қажет құрылғының мекенжайын көрсетіңіз.

     Құрылғының мекенжайы ретінде IP мекенжайын, NetBIOS- немесе DNS атауын пайдалануға болады.

     Әдепкі бойынша, утилита іске қосылған контекстік мәзірден құрылғының мекенжайы көрсетіледі.

   - Құрылғыға қосылу үшін есептік жазбаны көрсетіңіз:

     - **Ағымдағы пайдаланушының атынан қосылу** (әдепкі бойынша таңдалған). Ағымдағы пайдаланушы есептік жазбасымен қосылыңыз.
     - **Қосылу кезінде қамтамасыз етілген пайдаланушы аты мен құпиясөзді пайдалану**. Көрсетілген есептік жазбамен қосылыңыз. Қажетті есептік жазбада **Пайдаланушы аты** мен **Құпиясөзін** көрсетіңіз.

     Құрылғыға қосылу құрылғының жергілікті әкімшісінің есептік жазбасында ғана мүмкін болады.

5. Егер утилитаның негізгі терезесінің бірінші өрісінде сіз **Басқару серверінің құралдары арқылы қатынасу** нұсқасын таңдасаңыз:

   - **Басқару сервері** өрісінде құрылғыға қосылу қажет Басқару серверінің мекенжайын көрсетіңіз.

     Сервердің мекенжайы ретінде IP мекенжайын, NetBIOS- немесе DNS атауын пайдалануға болады.

     Әдепкі бойынша, утилита іске қосылатын Сервердің мекенжайы көрсетілген.

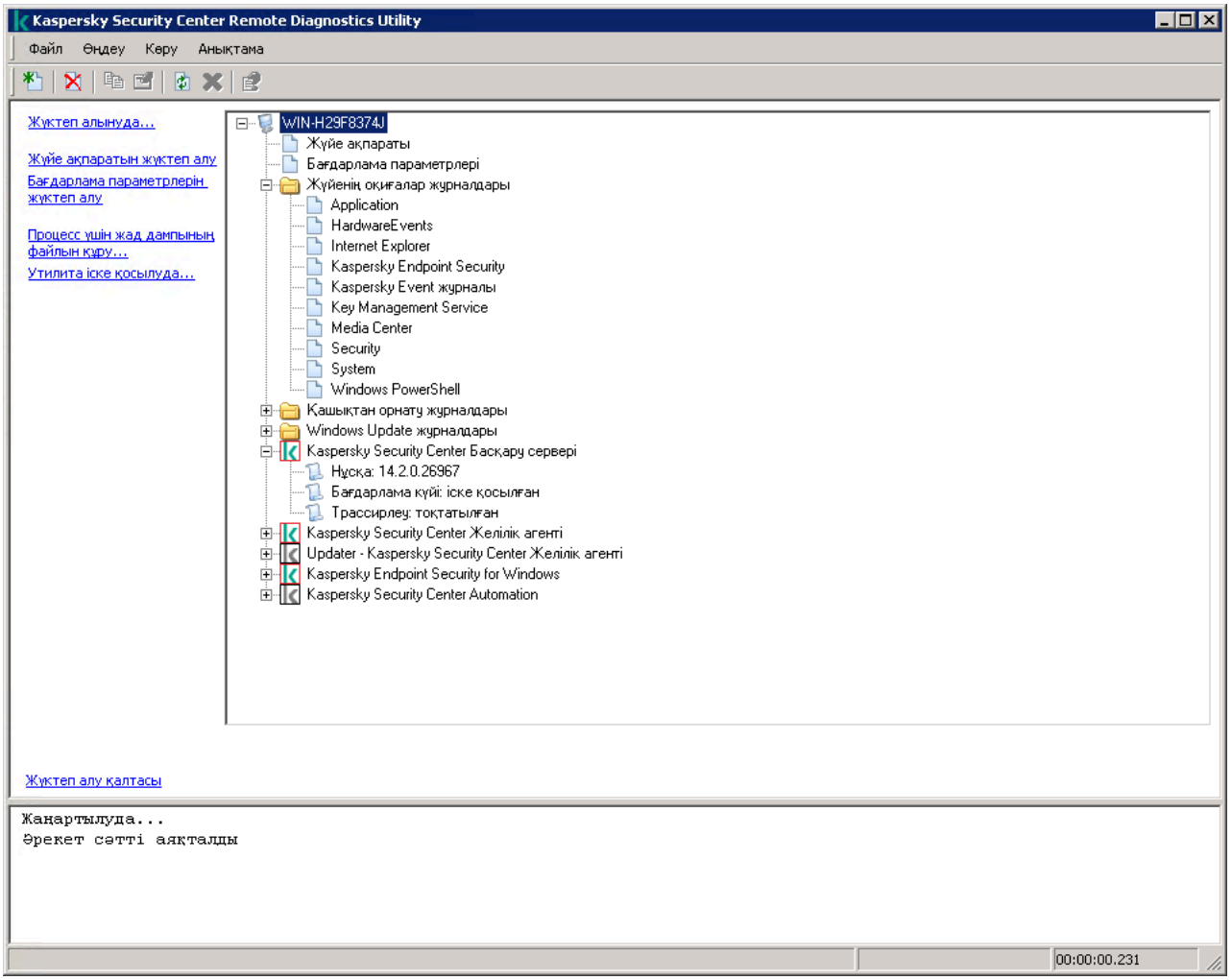
   - Қажет болса, **SSL пайдалану**, **Трафикті сығу** және **Құрылғы қосалқы Басқару серверінің иелігінде** жалаушаларын қойыңыз.

     Құрылғы қосалқы Басқару серверінің иелігінде жалаушасы қойылған болса, **Құрылғы қосалқы Басқару серверінің иелігінде** өрісінде **Шолу** түймесін басып, құрылғыны басқаратын қосалқы Басқару серверін таңдай аласыз.

6. Құрылғыға қосылу үшін **Кіру** түймесін басыңыз.

Есептік жазбаңыз үшін екі қадамдық тексеру қосылса, екі қадамдық тексеру арқылы авторизациялауыңыз керек.

Нәтижесінде, құрылғыны қашықтан диагностикалау терезесі ашылады (төмендегі суретті қараңыз). Терезенің сол жағында құрылғыны диагностикалау операцияларын орындау үшін сілтемелер бар. Терезенің оң жағында утилита жұмыс істей алатын құрылғы нысандарының ағашы орналасқан. Терезенің төменгі жағында утилита операцияларын орындау процесі көрсетіледі.



Қашықтан диагностикалау утилитасы. Құрылғыны қашықтан диагностикалау терезесі

Қашықтан диагностикалау утилитасы құрылғылардан жүктелген файлдарды ол іске қосылған құрылғының жұмыс үстелінде сақтайды.

Бағдарламадан алынған қоқыс файлын жасау

Бағдарламадан алынған қоқыс файлы белгілі бір уақытта клиент құрылғысында жұмыс істейтін бағдарламаның параметрлерін көруге мүмкіндік береді. Бұл файлда бағдарлама үшін жүктелген модульдер туралы ақпарат та бар.

Linux операциялық жүйесі бар клиент құрылғыларынан дамп файлдарын шығарып алуға қолдау көрсетілмейді.

Қашықтағы диагностика арқылы дамп файлдарын алу үшін kldumper утилитасы қолданылады. Бұл утилита Техникалық қолдау қызметі мамандарының сұрауы бойынша Kaspersky бағдарламаларының технологиялық дамп файлдарын алуға арналған. kldumper утилитасын пайдалану талаптары туралы толық ақпарат Kaspersky Security Center білім қорында берілген.

Бағдарламаға арналған қоқыс файлын жасау үшін:

1. **Басқарылатын құрылғылар** қалтасының жұмыс аймағындағы **Құрылғылар** қойындысында қажетті құрылғының контекстік мәзірінен **Реттелмелі құралдар → Қашықтан диагностикалау** тармағын таңдаңыз.

   Kaspersky Security Center Remote Diagnostics Utility терезесі ашылады.

2. Қашықтан диагностикалау утилитасын клиент құрылғысына қосыңыз.

   Нәтижесінде құрылғыны қашықтан диагностикалау терезесі ашылады.

3. Терезенің оң жағындағы **Процесс үшін жад дампының файлын құру** сілтемесіне өтіңіз.

4. Ашылған **Процестің дамп файлы жасалуда** терезесінде қоқыс файлын жасағыңыз келетін бағдарламаның орындалатын файлын көрсетіңіз.

5. **OK** түймесін басыңыз.

   Көрсетілген бағдарлама үшін дамп файлы бар мұрағат жүктелді.

   Көрсетілген бағдарлама клиент құрылғысында жұмыс істемесе, жүктелген мұрағаттағы "result" қалтасы бос болады.

   Көрсетілген қолданба жұмыс істеп тұрса, бірақ жүктеп алу қатемен сәтсіз аяқталса немесе жүктеп алынған мұрағаттағы "нәтиже" қалтасы бос болса, Kaspersky Security Center білім қорын қараңыз.

Трассалауды қосу және өшіру, трассалау файлын жүктеу

Қашықтағы құрылғыда трассалауды қосу үшін:

1. Қашықтан диагностикалау утилитасын іске қосып, өзіңізге қажетті құрылғыға қосылыңыз.

2. Құрылғы нысандары шежіресінде, трассалауды қосуды қажет ететін бағдарламаны таңдаңыз.

   Өзін-өзі қорғайтын бағдарламаларда трассалауды қосу және өшіру тек құрылғыға Басқару серверінің құралдарымен қосылған кезде ғана мүмкін болады.

Желілік агент үшін трассалауды қосқыңыз келсе, мұны Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау кезінде де орындай аласыз. Бұл жағдайда, қашықтан диагностикалау утилитасындағы Желілік агент үшін трассалау өшірулі болса да, Желілік агент трассалауды жазады.

3. Трассалауды қосу үшін:

   a. Қашықтан диагностикалау утилитасы терезесінің сол жағында **Трассирлеуді қосу** түймесін басыңыз.

   b. Ашылған **Трассирлеу деңгейін таңдау** терезесінде әдепкі бойынша белгіленген мәндерді өзгертпеу ұсынылады. Қажет болса, Техникалық қолдау қызметінің маманы сізді конфигурациялау процесі арқылы өткізеді. Келесі параметрлер қолжетімді:

      - **Трассирлеу деңгейі**

        Трассалау деңгейі, трассалау файлындағы ақпарат құрамын анықтайды.

      - **Айналдыру негізіндегі трассирлеу** (тек Kaspersky Endpoint Security үшін қолжетімді)

        Бағдарлама трассалау файлының шамадан тыс ұлғаюына жол бермеу үшін трассалау ақпаратын қайта жазады. Трассалау ақпаратын сақтау үшін пайдаланылатын файлдардың ең көп санын және әр файлдың ең үлкен өлшемін көрсетіңіз. Ең үлкен өлшемдегі трассирлеу файлдарының ең көп саны жазылған болса, ең ескі трассирлеу файлы жойылады, осылайша жаңа трассирлеу файлын жазуға болады.

   c. **OK** түймесін басыңыз.

4. Kaspersky Endpoint Security үшін Техникалық қолдау қызметінің мамандары жүйенің өнімділігі туралы ақпарат алу үшін сізден Xperf трассалауын қосуыңызды сұрауы мүмкін.

   Xperf трассалауын қосу үшін:

   a. Қашықтан диагностикалау утилитасы терезесінің сол жағында **Xperf трассирлеуді қосу** түймесін басыңыз.

   b. Ашылған **Трассирлеу деңгейін таңдау** терезесінде, Техникалық қолдау қызметі маманының сұрауына байланысты, келесі трассалау деңгейлерінің бірін таңдаңыз:

      - **Жеңіл деңгей**

        Бұл түрдегі трассирлеу файлы жүйе туралы ақпараттың ықшам өлшемін қамтиды.

        Әдепкі бойынша, осы нұсқа таңдалған.

      - **Күрделі деңгей**

        Бұл түрдегі трассалау файлы *Жеңіл деңгей* типті файлдан да егжей-тегжейлі ақпаратты қамтиды және *жеңіл деңгейлі* трассалау файлындағы ақпарат өнімділікті бағалау үшін жеткіліксіз болса, Техникалық қолдау қызметінің мамандары тарапынан сұралуы мүмкін. *Егжей-тегжейлі деңгейдегі* трассирлеу файлы жабдық, операциялық жүйе туралы ақпаратты, іске қосылған және аяқталған процестер мен бағдарламалардың тізімін, өнімділікті бағалау үшін пайдаланылатын оқиғаларды және Windows жүйесін бағалау құралының оқиғаларын қамтиды.

   c. Трассалау деңгейлерінің бірін таңдаңыз:

      - **Негізгі түрі**

        Бағдарлама трассалау деректерін Kaspersky Endpoint Security бағдарламасы жұмыс істеп тұрған кезде алады.

        Әдепкі бойынша, осы нұсқа таңдалған.

- **Қайта бастау түрі**

  Бағдарлама, басқарылатын құрылғыда операциялық жүйе іске қосылған кезде трассалау деректерін алады. Осы трассалау түрі, жүйенің өнімділігіне әсер ететін мәселе құрылғыны қосқаннан кейін және Kaspersky Endpoint Security іске қосылмай тұрып пайда болған кезде тиімді болады.

d. Сондай-ақ, трассалау файлының шамадан тыс ұлғаюына жол бермеу үшін **Айналдыру негізіндегі трассирлеу** параметрін қосу ұсынылуы мүмкін. Трассалау файлының ең үлкен өлшемін көрсетіңіз. Файл ең үлкен өлшемге жеткенде, ең ескі трассирлеу файлы жаңа файлмен алмастырылып, қайта жазылады.

e. **OK** түймесін басыңыз.

Кейбір жағдайларда, қауіпсіздік бағдарламасын трассалауды қосу үшін осы бағдарламаны және оның тапсырмасын қайта іске қосу қажет.

Қашықтан диагностикалау утилитасы таңдалған бағдарлама үшін трассалауды алуға мүмкіндік береді.

Бағдарламаны трассирлеу файлын жүктеп алу үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.
2. **Файлдарды трассирлеу** қалтасындағы бағдарламаның түйінінде қажетті файлды таңдаңыз.
3. Қашықтан диагностикалау утилитасы терезесінің сол жағында **Бүкіл файлды жүктеп алу** түймесін басыңыз.

   Үлкен көлемді файлдар үшін трассалаудың соңғы бөліктерін ғана жүктеу мүмкіндігі бар.

   Бөлектелген трассалау файлын жоюыңызға болады. Файл, трассалау өшірілгеннен кейін ғана жойылуы мүмкін.

Таңдалған файл терезенің төменгі жағында көрсетілген орналасқан жерге жүктеледі.

Қашықтағы құрылғыда трассалауды өшіру үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.
2. Құрылғының нысандары шежіресінде трассалауды өшіру қажет болған бағдарламаны таңдаңыз.

   Өзін-өзі қорғайтын бағдарламаларда трассалауды қосу және өшіру тек құрылғыға Басқару серверінің құралдарымен қосылған кезде ғана мүмкін болады.

3. Қашықтан диагностикалау утилитасы терезесінің сол жағында **Трассирлеуді өшіру** түймесін басыңыз.

Қашықтан диагностикалау утилитасы таңдалған бағдарлама үшін трассалауды өшіреді.

Бағдарламалар параметрлерін жүктеу

Қашықтағы құрылғыдан бағдарлама параметрлерін жүктеу үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.

2. Қашықтан диагностикалау утилитасы терезесі нысандары шежіресінде құрылғы атауы бар жоғарғы түйінді таңдаңыз.

3. Қашықтан диагностикалау утилитасы терезесінің сол жағында келесі параметрлерден қажетті әрекетті таңдаңыз:

   - **Жүйе ақпаратын жүктеп алу**
   - **Бағдарлама параметрлерін жүктеп алу**
   - **Процесс үшін жад дампының файлын құру**

     Осы сілтеме бойынша ашылған терезеде қоқыс файлын қалыптастыру қажет болған бағдарламаның орындалатын файлын көрсетіңіз.

   - **Утилита іске қосылуда**

     Осы сілтеме бойынша ашылған терезеде іске қосқыңыз келетін утилитаның орындалатын файлын және оны іске қосу параметрлерін көрсетіңіз.

Нәтижесінде, таңдалған утилита құрылғыға жүктеледі және онда жұмыс іске қосылады.

Оқиғалар журналдарын жүктеу

Қашықтағы құрылғыдан оқиғалар журналын жүктеу үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.

2. Құрылғылар нысаны шежіресіндегі **Жүйенің оқиғалар журналдары** қалтасында тиісті оқиғалар журналын таңдаңыз.

3. Оқиғалар журналын жүктеу үшін, қашықтан диагностикалау утилитасы терезесінің сол жақ бөлігінде **<Оқиғалар журналының атауы> оқиғалар журналын іске қосу** сілтемесі бойынша өтіңіз.

Таңдалған оқиғалар журналы терезенің төменгі жағында көрсетілген орналасқан жерге жүктеледі.

Бірнеше диагностикалық ақпараттық элементтерді жүктеу

Kaspersky Security Center қашықтан диагностикалау утилитасы диагностикалық ақпараттың бірнеше элементтерін, соның ішінде оқиғалар журналдарын, жүйелік ақпаратты, трассалау файлдарын және қоқыс файлдарын жүктеуге мүмкіндік береді.

Қашықтағы құрылғыдан диагностикалық ақпаратты жүктеу үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.
2. Қашықтан диагностикалау утилитасы терезесінің сол жағында **Жүктеп алынуда** түймесін басыңыз.
3. Жүктеп алғыңыз келетін нысандарға қарсы жалаушаны қойыңыз.
4. **Іске қосу** түймесін басыңыз.

Әрбір таңдалған нысан төменгі тақтада көрсетілген орналасқан жерге жүктеледі.

Диагностиканы іске қосу және оның нәтижелерін жүктеу

Қашықтағы құрылғыда бағдарламаның диагностикасын іске қосу және оның нәтижелерін жүктеу үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.
2. Құрылғы нысандары шежіресінде қажетті бағдарламаны таңдаңыз.
3. Диагностиканы іске қосу үшін қашықтан диагностикалау утилитасы терезесінің сол жағындағы **Диагностиканы іске қосу** сілтемесі бойынша өтіңіз.

   Нәтижесінде, нысандар шежіресінде таңдалған бағдарламаның түйінінде диагностикалық есеп пайда болады.
4. Нысандар шежіресінде қалыптасқан диагностикалық есепті таңдап, оны **Жүктеп алу қалтасы** сілтемесі бойынша жүктеп алыңыз.

Таңдалған есеп терезенің төменгі жағында көрсетілген орналасқан жерге жүктеледі.

Бағдарламаларды іске қосу, тоқтату және қайта іске қосу

Бағдарламаларды іске қосу, тоқтату және қайта қосу құрылғыға Басқару сервері құралдарымен қосылған кезде ғана мүмкін болады.

Бағдарламаны іске қосу, тоқтату және қайта қосу үшін:

1. Қашықтан диагностикалау утилитасын іске қосыңыз және "Қашықтан диагностикалау утилитасын клиент құрылғысына қосу" бөлімінде сипатталғандай қажетті құрылғыға қосылыңыз.
2. Құрылғы нысандары шежіресінде қажетті бағдарламаны таңдаңыз.

3. Қашықтан диагностикалау утилитасы терезесінің сол жағында әрекетті таңдаңыз:

   - **Бағдарламаны тоқтату**
   - **Бағдарламаны қайта іске қосу**
   - **Бағдарламаны іске қосу**

Өзіңіз таңдаған әрекетке байланысты, бағдарлама іске қосылады, тоқтайды немесе қайта іске қосылады.

UEFI деңгейлі қорғанысты құрылғылар

UEFI деңгейлі қорғанысты құрылғы – бұл BIOS деңгейінде кіріктірілген, UEFI үшін "Kaspersky" шешімі немесе бағдарламасы бар құрылғы. Кіріктірілген қорғаныс жүйені іске қосуды бастаған сәттен бастап құрылғының қауіпсіздігін қамтамасыз етеді, ал кіріктірілген БҚ жоқ құрылғылар қорғанысы тек қауіпсіздік бағдарламасы іске қосылғаннан кейін ғана әрекет ете бастайды. Kaspersky Security Center бағдарламасы осындай құрылғыларды басқаруға қолдау көрсетеді.

UEFI деңгейлі қорғанысты құрылғыларын қосу параметрлерін өзгерту үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде **Сервермен байланыс параметрлері → Қосымша порттар** бөлімін таңдаңыз.
4. **Қосымша порттар** бөлімінде өзіңізге қажетті параметрлерді өзгертіңіз:

   - **UEFI деңгейлі қорғанысты және KasperskyOS құрылғылары үшін портты ашу**

     UEFI деңгейлі қорғанысты құрылғылар Басқару серверіне қосыла алады.

   - **UEFI деңгейлі қорғанысты және KasperskyOS құрылғыларына арналған порт**

     UEFI деңгейлі қорғанысты және KasperskyOS құрылғылары үшін портты ашу нұсқасы таңдалса, порт нөмірін өзгертуге болады. Әдепкі бойынша 13294-порт орнатылған.

5. **OK** түймесін басыңыз.

Басқарылатын құрылғының параметрлері

Басқарылатын құрылғының параметрлерін қарап шығу үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында құрылғыны таңдаңыз.
3. Құрылғының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.

Жалпы бөлімі таңдалған құрылғы сипаттары терезесі ашылады.

Жалпы

Жалпы бөлімі клиент құрылғысы туралы жалпы ақпаратты қамтиды. Ақпарат, клиент құрылғысын Басқару серверімен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады:

- **Атауы**

  Өрісте басқару тобындағы клиент құрылғысының атауын қарап шығуға және өзгертуге болады.

- **Сипаттама**

  Өрісте клиент құрылғысының қосымша сипаттамасын енгізуге болады.

- **Windows домені**

  Windows домені немесе құрылғы кіретін жұмыс тобы.

- **NetBIOS атауы**

  Windows желісіндегі клиент құрылғысының атауы.

- **DNS атауы**

  Клиент құрылғысының DNS домен атауы.

- **IP мекенжайы**

  Құрылғының IP мекенжайы.

- **Топ**

  Құрамына клиент құрылғысы кіретін басқару тобы.

- **Соңғы рет жаңартылған уақыты**

  Құрылғыдағы антивирустық дерекқорларды немесе бағдарламаларды соңғы рет жаңарту күні.

- **Байланысқа соңғы рет шығу уақыты**

  Құрылғы соңғы рет желіде көрінген күн мен уақыт.

- **Басқару серверіне қосылған уақыты**

  Клиент құрылғысында орнатылған Желілік агентті Басқару серверіне соңғы рет қосу күні мен уақыты.

- **Басқару серверімен байланысты үзбеу**

  Осы параметрі қосулы болса, басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылым сақталады. Осындай қосылымды қамтамасыз ететін push-серверлерді қолданбасаңыз, осы параметрді қолдана аласыз.

  Егер параметр өшірулі болса және push серверлері пайдаланылмаса, басқарылатын құрылғы деректерді синхрондау немесе ақпаратты жіберу үшін Басқару серверіне қосылады.

  Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың жалпы саны 300-ден аспауы тиіс.

  Бұл параметр басқарылатын құрылғыларда әдепкі бойынша өшіріледі. Бұл параметр Басқару сервері орнатылған құрылғыда әдепкі бойынша қосылады және оны өшіруге тырыссаңыз да қосулы қалады.

Қорғаныс

Қорғаныс бөлімінде клиент құрылғысында антивирустық қорғаныстың күйі туралы ақпарат ұсынылған:

- **Құрылғының күйі**

  Құрылғыдағы антивирустық қорғаныс күйінің және желідегі құрылғы белсенділігінің әкімші белгілеген өлшемшарттары негізінде қалыптастырылатын клиент құрылғысының күйі.

- **Барлық мәселелер**

  Бұл кестеде клиент құрылғысында орнатылған басқарылатын бағдарламалар анықтаған мәселелердің толық тізімі бар. Әрбір мәселе басқарылатын бағдарлама осы мәселеге байланысты құрылғыны тағайындауды ұсынатын күйге ие.

- **Нақты уақыт режимінде қорғау**

  Клиент құрылғысынның тұрақты қорғанысының ағымдағы күйі.

  Құрылғыда күй өзгергеннен кейін, жаңа күй, клиент құрылғысы Басқару серверімен синхрондалғаннан кейін ғана құрылғының сипаттары терезесінде көрсетіледі.

- **Талап бойынша соңғы сканерлеу**

  Клиент құрылғысында зиянды БҚ соңғы іздеу күні мен уақыты.

- **Анықталған қауіптердің жалпы саны**

  Қауіпсіздік бағдарламасын орнатқан сәттен бастап (құрылғыны бірінші рет тексеру) немесе қауіп есептегіші соңғы нөлденген сәттен бастап клиент құрылғысында анықталған қауіптердің жалпы саны.

- **Белсенді қауіптер**

  Клиент құрылғысындағы кейін өңделетін файлдар саны.

  Өрісте ұялы құрылғылар үшін кейін өңделетін файлдар ескерілмейді.

- **Дискілерді шифрлау күйі**

  Құрылғының жергілікті дискілеріндегі файлдарды шифрлаудың ағымдағы күйі. Күйдің сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

Бағдарламалар

Бағдарламалар бөлімінде клиент құрылғысында орнатылған Kaspersky бағдарламаларының тізімі көрсетілед. Бұл бөлімде, таңдалған Kaspersky қолданбасын (Желілік агенттен басқа) іске қосуға және тоқтатуға мүмкіндік беретін бастау () түймесі және тоқтату () түймесі бар. Басқару серверінен push хабарландыруларын алу үшін басқарылатын құрылғыларда 15000 UDP порты қолжетімді болса, бұл түймелер қолжетімді болады. Басқарылатын құрылғы push хабарландырулары үшін қолжетімді болмаса, бірақ Басқару серверіне тұрақты қосылу режимі қосылған болса (**Жалпы** бөліміндегі **Басқару серверімен байланысты үзбеу** параметрі қосылған), бастау және тоқтату түймелері белсенді болады. Сондай-ақ, **Бағдарламалар** бөлімінде келесі түймелер де бар:

- **Оқиғалар**

Түймені басқан кезде, сіз бағдарлама жұмыс істеп тұрған кезде клиент құрылғысында болған оқиғалардың тізімін, сондай-ақ осы бағдарламаның тапсырмаларын орындау нәтижелерін көре аласыз.

- **Статистика**

  Түймені басқан кезде бағдарламаның жұмысы туралы ағымдағы статистикалық ақпаратты көруге болады.

- **Сипаттар**

  Түймені басқан кезде бағдарлама туралы ақпарат алуға және бағдарламаны конфигурациялауға болады.

Тапсырмалар

Тапсырмалар қойындысында клиент құрылғысының тапсырмаларын басқара аласыз: қолданыстағы тапсырмалар тізімін қарау, жаңаларын жасау, тапсырмаларды жою, іске қосу және тоқтату, олардың параметрлерін өзгерту және орындау нәтижелерін қарау. Тапсырмалар тізімі клиентті Басқару серверімен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады. Тапсырмалардың күйі туралы ақпаратты клиент құрылғысынан Басқару сервері сұрайды.

Басқару серверінен push хабарландыруларын алу үшін басқарылатын құрылғыларда 15000 UDP порты қолжетімді болса, бастау (), тоқтату () және жою () түймелері қолжетімді болады. Басқарылатын құрылғы push хабарландырулары үшін қолжетімді болмаса, бірақ Басқару серверіне тұрақты қосылу режимі қосылған болса (**Басқару серверімен байланысты үзбеу** бөліміндегі **Жалпы** параметрі қосылған), бастау, тоқтату және жою түймелері белсенді болады.

Қосылым болмаса, тапсырма күйі көрсетілмейді және түймелер белсенді емес.

Оқиғалар

Оқиғалар қойыншасында таңдалған клиент құрылғысы үшін Басқару серверінде тіркелген оқиғалар көрсетіледі.

Құрылғылар оқиғаларын экспорттауға, көшіруге және жоюға болады.

Тегтер

Тегтер қойыншасында клиент құрылғысын іздеуге негізделген кілт сөздер тізімін басқаруға болады: қолданыстағы тегтер тізімін қарау, тізімнен тегтер тағайындау, автоматты түрде тег қою ережелерін конфигурациялау, жаңа тегтер қосу және ескі тегтердің атын өзгерту, тегтерді жою.

Жүйе ақпараты

Жалпы жүйе ақпараты бөлімінде клиент құрылғысында орнатылған бағдарлама туралы ақпарат ұсынылған.

Бағдарламалар тізімдемесі

Бағдарламалар тізімдемесі бөлімінде клиент құрылғысында орнатылған бағдарламалар мен оларға арналған жаңартулардың тізімдемесін көруге, сондай-ақ бағдарламалар тізімдемесінің көрсетілуін конфигурациялауға болады.

Орнатылған бағдарламалар туралы ақпарат, клиент құрылғысында орнатылған Желілік агент қажетті ақпаратты Басқару серверіне берген жағдайда беріледі. Басқару серверіне ақпаратты беру параметрлерін **Қоймалар** бөліміндегі Желілік агент сипаттары немесе оның саясаты конфигурациялауға болады.

- **Тек үйлесімсіз қауіпсіздік бағдарламаларын көрсету**

  Егер параметр қосылса, бағдарламалар тізімінде тек Kaspersky бағдарламаларына сәйкес келмейтін қауіпсіздік бағдарламалары көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартуларды көрсету**

  Егер параметр қосылса, бағдарламалар тізімінде тек бағдарламалар ғана емес, олар үшін орнатылған жаңарту пакеттері де көрсетіледі.

  Жаңартулар тізімін көрсету үшін сізге 100 КБ трафик қажет. Егер сіз тізімді жауып, оны қайта ашсаңыз, сізге 100 КБ трафик жұмсауға тура келеді.

  Әдепкі бойынша, параметр өшірулі.

- **Файлға экспортталуда**

  Құрылғыда орнатылған бағдарламалар тізімін CSV не TXT пішіміндегі файлға экспорттау үшін осы түймені басыңыз.

- **Журнал**

  Бағдарламаларды құрылғыға орнатуға қатысты оқиғаларды көру үшін осы түймені басыңыз. Келесі ақпарат көрсетіледі:

  - Бағдарлама құрылғыға орнатылған күн мен уақыт
  - Бағдарлама атауы
  - Бағдарлама нұсқасы

- **Сипаттар**

  Құрылғыда орнатылған бағдарламалар тізімінен таңдалған бағдарламаның сипаттарын көру үшін осы түймені басыңыз. Келесі ақпарат көрсетіледі:

  - Бағдарлама атауы
  - Бағдарлама нұсқасы
  - Бағдарламаны өндіруші

Орындалатын файлдар

Орындалатын файлдар бөлімінде клиент құрылғысында табылған орындалатын файлдар көрсетіледі.

Жабдық тізімдемесі

Жабдық тізімдемесі бөлімінде клиент құрылғысында орнатылған жабдық туралы ақпаратты көруге болады. Бұл ақпаратты Windows және Linux операциялық жүйелері бар құрылғылар үшін көруге болады.

lshw утилитасы, жабдық туралы ақпарат алғыңыз келетін Linux құрылғыларында орнатылғанын тексеріңіз. Виртуалды машиналардан алынған жабдық туралы мәлімет пайдаланылатын гипервизорға байланысты толық болмауы мүмкін

Желілік агент Windows жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді:

- ЖЖҚ
- Жаппай сақтау құрылғылары
- Негізгі тақта
- Процессор
- Желілік адаптерлер
- Мониторлар
- Бейне адаптері
- Дыбыстық карта

Желілік агент Linux немесе macOS жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді (бұл ақпаратты операциялық жүйе қамтамасыз етсе):

- Жалпы ЖЖҚ көлемі
- Жаппай сақтау құрылғыларының жалпы көлемі
- Негізгі тақта
- Процессор
- Желілік адаптерлер

Сеанстар

Сеанстар бөлімінде тек Windows жүйесімен жұмыс істейтін құрылғылар үшін ақпарат берілген және клиент құрылғысының иесі, сондай-ақ таңдалған клиенттік құрылғымен жұмыс істеген пайдаланушы есептік жазбалары туралы ақпарат қамтылған.

Домендік пайдаланушылар туралы ақпарат Active Directory деректері негізінде құрылады. Жергілікті пайдаланушылар туралы ақпаратты клиент құрылғысында орнатылған қауіпсіздік есептік жазбаларының диспетчері (Security Account Manager) ұсынады.

- **Құрылғының иесі**

  Құрылғының иесі өрісінде клиент құрылғысымен қандай да бір жұмысты орындау қажет болған жағдайда әкімші байланыса алатын пайдаланушы аты көрсетіледі.

  Тағайындау және **Сипаттар** түймелері бойынша құрылғы иесін таңдауға және құрылғының иесі тағайындаған пайдаланушы туралы мәліметті қарауға болады.

  Қызыл кіресі бар түймесі арқылы құрылғының ағымдағы иесін жоюға болады.

Тізімде клиент құрылғысымен жұмыс істеп жатқан пайдаланушылардың есептік жазбалары бар.

- **Атауы**

  Windows желісіндегі құрылғының атауы.

- **Қатысушының аты**

  Осы құрылғыға кірген пайдаланушы аты (домендік немесе жергілікті).

- **Есептік жазба**

  Осы құрылғыға кірген пайдаланушының есептік жазбасы.

- **Электрондық пошта**

  Пайдаланушының электрондық пошталары.

- **Телефон**

  Пайдаланушының телефон нөмірі.

Қауіпсіздік мәселелері

Қауіпсіздік мәселелері қойындысында клиенттік құрылғы үшін қауіпсіздік мәселелерін көруге, өңдеуге және жасауға болады. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін. Мысалы, кейбір пайдаланушылар зиянды бағдарламаны алынбалы жетектерден құрылғыларға жүйелі түрде жылжытса, әкімші қауіпсіздік мәселесін жасай алады. Әкімші қауіпсіздік мәселесі мәтінінде пайдаланушыға қарсы жасалуы керек жағдай мен ұсынылған әрекеттердің қысқаша сипаттамасын (мысалы, тәртіптік іс-әрекеттер) көрсете алады және пайдаланушыға не пайдаланушыларға сілтеме қоса алады.

Қажетті әрекеттер орындалған қауіпсіздік мәселесі *өңделген* деп аталады. Өңделмеген қауіпсіздік мәселелерінің болуы құрылғының күйін *Критикалық* немесе *Ескерту* күйіне өзгерту шарты ретінде таңдалуы мүмкін.

Бөлімде құрылғы үшін жасалған қауіпсіздік мәселелерінің тізімі берілген. Қауіпсіздік мәселелері маңыздылық деңгейі мен түріне қарай жіктеледі. Қауіпсіздік мәселесінің түрі қауіпсіздік мәселесін жасайтын Kaspersky қолданбасы арқылы анықталады. Өңделген қауіпсіздік мәселелерін **Өңделген** бағанына жалауша қою арқылы тізімде белгілеуге болады.

Бағдарламалық жасақтама осалдықтары

Бағдарламалық жасақтама осалдықтары бөлімінде клиент құрылғыларында орнатылған үшінші тарап бағдарламаларының осалдығы туралы ақпарат бар тізімді көруге болады. Тізімнің үстіндегі іздеу жолын пайдаланып, осалдық тізімінен осалдық атауы бойынша іздеуге болады.

- **Файлға экспортталуда**

  Файлға экспорттау түймесі бойынша осалдықтар тізімін файлға сақтауға болады. Әдепкі бойынша, бағдарлама осалдықтар тізімін CSV пішіміндегі файлға экспорттайды.

- **Тек түзетуге болатын осалдықтарды көрсету**

  Егер параметр қосулы болса, бөлімде патчпен жабуға болатын осалдықтар көрсетіледі.

  Параметр өшірулі болса, бөлімде патчпен жабуға болатын осалдықтар да, патч жоқ осалдықтар да көрсетіледі.

  Әдепкі бойынша, параметр қосулы.

- **Сипаттар**

  Тізімдегі бағдарламалардағы осалдықты таңдап, таңдалған осалдық сипаттарын бөлек терезеде бағдарламаларда көру үшін **Сипаттар** түймесін басыңыз. Сипаттар терезесінде келесі әрекеттерді орындауға болады:

  - Осы басқарылатын құрылғыдағы бағдарламаларда (Басқару консолінде немесе Kaspersky Security Center Web Console веб-консолінде) осалдықты өткізіп жіберу.
  - Осалдық үшін ұсынылған түзетулер тізімін қарап шығу.
  - Осалдықты түзету үшін бағдарламалық жасақтама жаңартуын қолмен көрсету (Басқару консолінде немесе Kaspersky Security Center Web Console веб-консолінде).
  - Осалдықтардың даналарын қарап шығу.
  - Осалдықты жабу үшін бар тапсырмалар тізімін қарап шығу және осалдықты жабу үшін тапсырмалар жасау.

Қолдануға болатын жаңартулар

Бұл бөлімде құрылғыда орнатылмаған бағдарламалық жасақтама жаңартуларының тізімін көруге болады. Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Орнатылған жаңартуларды көрсету**

  Егер параметр қосулы болса, жаңартулар тізімінде орнатылмаған жаңартулар да, клиенттік құрылғыда орнатылған жаңартулар да көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

Белсенді саясаттар

Бұл бөлімде қазіргі уақытта құрылғыға тағайындалған Kaspersky бағдарламаларына арналған саясаттар тізімі көрсетілген.

- **Файлға экспортталуда**

  Файлға экспорттау түймесі бойынша белсенді саясаттар тізімін файлға сақтауға болады. Әдепкі бойынша, бағдарлама саясаттар тізімін CSV пішіміндегі файлға экспорттайды.

Белсенді саясат профильдері

- **Белсенді саясат профильдері**

  Тізімде клиент құрылғыларында белсенді болатын қолданыстағы саясат профильдері туралы мәліметті көруге болады. Тізімнің үстіндегі іздеу жолын пайдаланып, тізімде саясаттың атауы немесе саясат профилінің атауы бойынша белсенді саясат профильдерін іздеуге болады.

- **Файлға экспортталуда**

  Файлға экспорттау түймесі бойынша белсенді саясат профильдері тізімін файлға сақтауға болады. Әдепкі бойынша, бағдарлама саясат профильдері тізімін CSV пішіміндегі файлға экспорттайды.

Тарату нүктелері

Бұл бөлімде құрылғы өзара әрекеттесетін тарату нүктелерінің тізімі берілген.

- **Файлға экспортталуда**

  Файлға экспорттау түймесі арқылы сіз құрылғы өзара әрекеттесетін тарату нүктелерінің тізімін файлға сақтай аласыз. Әдепкі бойынша, бағдарлама құрылғылар тізімін CSV пішіміндегі файлға экспорттайды.

- **Сипаттар**

  Сипаттар түймесі арқылы құрылғы өзара әрекеттесетін тарату нүктесінің параметрлерін көруге және конфигурациялауға болады.

Саясаттардың жалпы параметрлері

Жалпы

Жалпы бөлімінде саясаттың күйін өзгертуге және саясат параметрлерін иеленуді конфигурациялауға болады:

- **Саясаттың күйі** блогында саясаттың әрекет ету ауқымы нұсқаларының біреуін таңдауға болады:
  - **Белсенді саясат**

    Осы нұсқа таңдалған болса, саясат белсенді болады.

    Әдепкі бойынша, осы нұсқа таңдалған.
  - **Автономды пайдаланушылар саясаты**

    Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.
  - **Белсенді емес саясат**

    Егер бұл нұсқа таңдалса, саясат белсенді болмайды, бірақ **Саясат** қалтасында сақталады. Қажет болса, оны белсенді етуге болады.
- **Параметрлерді иелену** блогында саясатты иелену параметрлерін конфигурациялауға болады:
  - **Параметрлерді негізгі саясаттан иелену**

    Параметр қосулы болса, саясат параметрлері мәндері иерархияның жоғарғы деңгейіндегі топқа арналған саясаттан иеленеді және өзгерту үшін қолжетімді емес.

    Әдепкі бойынша, параметр қосулы.
  - **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену**

    Егер параметр қосылса, саясатқа өзгертулер қолданылғаннан кейін келесі қадамдар орындалады:
    - саясат параметрлерінің мәндері салынған басқару топтарының саясаты – еншілес саясаттарға қатысты қолданылады;
    - Әрбір еншілес саясат сипаттары терезесінің **Жалпы** бөлімінің **Параметрлерді иелену** блогында **Параметрлерді негізгі саясаттан иелену** параметрі автоматты түрде қосылады.

    Параметр қосулы болған кезде, еншілес саясат параметрлерінің мәндерін өзгерту қолжетімді емес.

    Әдепкі бойынша, параметр өшірулі.

Оқиғаларды конфигурациялау

Оқиғаларды конфигурациялау бөлімінде оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар қойыншалардағы маңыздылық деңгейлері бойынша бөлінген:

- **Критикалық**

  Критикалық қойыншасы Желілік агент саясатының сипаттарында көрсетілмейді.

- **Функционалдық ақау**
- **Ескерту**
- **Ақпараттық**

Әр қойыншада, оқиғалар түрлерінің тізімі және оқиғаларды әдепкі бойынша Басқару серверінде сақтау уақыты көрсетіледі (күндермен). **Сипаттар** түймесі бойынша тізімде таңдалған оқиғаларды тіркеу және хабарлау параметрлерін конфигурациялауға болады. Әдепкі бойынша, барлық Басқару сервері үшін көрсетілген жалпы хабарландыру конфигурациясы оқиғалардың барлық түрлері үшін қолданылады. Дегенмен, белгіленген оқиға түрлері үшін белгілі бір параметрлерді өзгертуге болады.

Ескерту қойыншасында **Қауіпсіздік мәселесі пайда болды** оқиғасының түрін конфигурациялауға болады. Мұндай оқиғалар, мысалы, тарату нүктесінің дискісіндегі бос орын 2 ГБ-тан аз болған кезде туындауы мүмкін (бағдарламаларды орнату және жаңартуларды қашықтан жүктеу үшін кемінде 4 ГБ қажет). **Қауіпсіздік мәселесі пайда болды** оқиғасын конфигурациялау үшін, оны таңдап, **Сипаттар** түймесін басыңыз. Осыдан кейін, сіз болған оқиғаларды қайда сақтау керектігін және олар туралы қалай хабарлау керектігін көрсете аласыз.

Желілік агент қауіпсіздік мәселесін анықтаса, сіз бұл қауіпсіздік мәселесін басқарылатын құрылғы параметрлері арқылы басқара аласыз.

Оқиғалардың бірнеше түрін таңдау үшін **SHIFT** немесе **CTRL** пернелерін пайдаланыңыз, барлық түрлерін таңдау үшін **Барлығын таңдау** түймесін пайдаланыңыз.

Желілік агент саясатының параметрлері

Желілік агент саясаты параметрлерін конфигурациялау үшін:

1. Консоль ағашында **Саясаттар** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағынан Желілік агент саясатын таңдаңыз.
3. Саясаттың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

Желілік агент саясатының сипаттары терезесі ашылады.

> Пайдаланылатын операциялық жүйе түріне байланысты төмендегі параметрлердің қалай қолданылатынын егжей-тегжейлі сипаттайтын салыстыру кестесін қараңыз.

Жалпы

Жалпы бөлімінде саясаттың күйін өзгертуге және саясат параметрлерін иеленуді конфигурациялауға болады:

- **Саясаттың күйі** блогында саясаттың әрекет ету ауқымы нұсқаларының біреуін таңдауға болады:
  - **Белсенді саясат**

    Осы нұсқа таңдалған болса, саясат белсенді болады.

    Әдепкі бойынша, осы нұсқа таңдалған.
  - **Автономды пайдаланушылар саясаты**

    Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.
  - **Белсенді емес саясат**

    Егер бұл нұсқа таңдалса, саясат белсенді болмайды, бірақ **Саясат** қалтасында сақталады. Қажет болса, оны белсенді етуге болады.
- **Параметрлерді иелену** блогында саясатты иелену параметрлерін конфигурациялауға болады:
  - **Параметрлерді негізгі саясаттан иелену**

    Параметр қосулы болса, саясат параметрлері мәндері иерархияның жоғарғы деңгейіндегі топқа арналған саясаттан иеленеді және өзгерту үшін қолжетімді емес.

    Әдепкі бойынша, параметр қосулы.
  - **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену**

    Егер параметр қосылса, саясатқа өзгертулер қолданылғаннан кейін келесі қадамдар орындалады:
    - саясат параметрлерінің мәндері салынған басқару топтарының саясаты – еншілес саясаттарға қатысты қолданылады;
    - Әрбір еншілес саясат сипаттары терезесінің **Жалпы** бөлімінің **Параметрлерді иелену** блогында **Параметрлерді негізгі саясаттан иелену** параметрі автоматты түрде қосылады.

    Параметр қосулы болған кезде, еншілес саясат параметрлерінің мәндерін өзгерту қолжетімді емес.

    Әдепкі бойынша, параметр өшірулі.

Оқиғаларды конфигурациялау

Оқиғаларды конфигурациялау бөлімінде оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар қойыншалардағы маңыздылық деңгейлері бойынша бөлінген:

- **Критикалық**

  Критикалық қойыншасы Желілік агент саясатының сипаттарында көрсетілмейді.
- **Функционалдық ақау**

- **Ескерту**
- **Ақпараттық**

Әр қойыншада, оқиғалар түрлерінің тізімі және оқиғаларды әдепкі бойынша Басқару серверінде сақтау уақыты көрсетіледі (күндермен). **Сипаттар** түймесі бойынша тізімде таңдалған оқиғаларды тіркеу және хабарлау параметрлерін конфигурациялауға болады. Әдепкі бойынша, барлық Басқару сервері үшін көрсетілген жалпы хабарландыру конфигурациясы оқиғалардың барлық түрлері үшін қолданылады. Дегенмен, белгіленген оқиға түрлері үшін белгілі бір параметрлерді өзгертуге болады.

Ескерту қойыншасында **Қауіпсіздік мәселесі пайда болды** оқиғасының түрін конфигурациялауға болады. Мұндай оқиғалар, мысалы, тарату нүктесінің дискісіндегі бос орын 2 ГБ-тан аз болған кезде туындауы мүмкін (бағдарламаларды орнату және жаңартуларды қашықтан жүктеу үшін кемінде 4 ГБ қажет). **Қауіпсіздік мәселесі пайда болды** оқиғасын конфигурациялау үшін, оны таңдап, **Сипаттар** түймесін басыңыз. Осыдан кейін, сіз болған оқиғаларды қайда сақтау керектігін және олар туралы қалай хабарлау керектігін көрсете аласыз.

Желілік агент қауіпсіздік мәселесін анықтаса, сіз бұл қауіпсіздік мәселесін басқарылатын құрылғы параметрлері арқылы басқара аласыз.

Оқиғалардың бірнеше түрін таңдау үшін **SHIFT** немесе **CTRL** пернелерін пайдаланыңыз, барлық түрлерін таңдау үшін **Барлығын таңдау** түймесін пайдаланыңыз.

Параметрлер

Параметрлер бөлімінде Желілік агент саясатының параметрлерін конфигурациялауға болады:

- **Файлдарды тек тарату нүктелері арқылы тарату**

  Егер бұл параметр қосылса, басқарылатын құрылғылардағы Желілік агенттер жаңартуларды тек тарату нүктелерінен алады.

  Егер бұл параметр өшірулі болса, басқарылатын құрылғылардағы Желілік агенттер тарату нүктелерінен немесе Басқару серверінен жаңартулар алады.

  > Басқарылатын құрылғылардағы қауіпсіздік бағдарламалары әрбір қауіпсіздік бағдарламасы үшін жаңарту тапсырмасында белгіленген көзден жаңартуларды алатынын ескеріңіз. **Файлдарды тек тарату нүктелері арқылы тарату** параметрін қоссаңыз, Kaspersky Security Center бағдарламасы жаңарту тапсырмаларында жаңарту көзі ретінде орнатылғанына көз жеткізіңіз.

  Әдепкі бойынша, параметр өшірулі.

- **Оқиғалар кезегінің максималды өлшемі, МБ**

  Өрісте оқиғалар кезегі болуы мүмкін дискідегі максималды орынды көрсетуге болады.

  Әдепкі бойынша, 2 МБ мәні көрсетілген.

- **Бағдарламаға құрылғыда саясаттың кеңейтілген деректерін шығарып алуға рұқсат берілген**

  Басқарылатын құрылғыға орнатылған Желілік агент, қолданылатын саясат туралы ақпаратты қауіпсіздік бағдарламасына жібереді (мысалы, Kaspersky Endpoint Security for Windows). Берілетін ақпарат қауіпсіздік бағдарламасының интерфейсінде көрсетіледі.

Желілік агент келесі ақпаратты береді:

- Саясатты басқарылатын құрылғыға жеткізу уақыты.
- Саясатты басқарылатын құрылғыға жеткізу кезінде белсенді саясат атауы.
- Басқарылатын құрылғыға саясатты жеткізу сәтіндегі кеңседен тыс саясаттың атауы (Linux жүйесіне арналған желілік агент үшін қолжетімді емес).
- Саясатты басқарылатын құрылғыға жеткізу кезінде басқарылатын құрылғыға тиесілі басқару тобының атауы және толық жолы.
- Басқарылатын құрылғыға саясатты жеткізу сәтіндегі атаулары мен басымдықтары бар белсенді саясат профильдерінің тізімі.

Бұл ақпаратты, құрылғыға дұрыс саясатты қолдануды қамтамасыз ету үшін және ақауларды жою мақсатында пайдалана аласыз. Әдепкі бойынша, параметр өшірулі.

- **Желілік агент қызметін рұқсатсыз өшіруден немесе тоқтатудан қорғау және параметрлердегі өзгерістердің алдын алу**

  Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, құрамдасты қажетті құқықтарсыз жою немесе өзгерту мүмкін емес. Желілік агенттің жұмысын тоқтату мүмкін емес. Бұл параметр домен контроллерлеріне әсер етпейді.

  Жергілікті әкімші құқықтарымен басқарылатын жұмыс станцияларында Желілік агентті қорғау үшін осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Жою құпиясөзін пайдалану**

  Егер параметр қосулы болса, **Өзгерту** түймесін басқан кезде, желілік агентті қашықтан жою тапсырмасы үшін klmover утилитасына арналған құпия сөзді көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

Қоймалар

Қоймалар бөлімінде желілік агенттен басқару серверіне жіберілетін нысандардың түрлерін таңдауға болады.

- **Windows Update жаңартулар мәліметтері**

  Егер параметр орнатылған болса, Windows Update жаңартулары туралы ақпарат клиент құрылғыларына орнатылуы керек Басқару серверіне жіберіледі.

  Кейде параметр өшірулі болса да, жаңартулар **Қолжетімді жаңартулар** бөліміндегі құрылғы сипаттарында көрсетіледі. Бұл, мысалы, ұйымның құрылғыларында осы жаңартулар арқылы жабылуы мүмкін осалдықтар болса, орын алуы мүмкін.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер**

  Егер бұл параметр қосылса, басқарылатын құрылғыларда табылған үшінші тарап бағдарламаларындағы (Microsoft бағдарламалық жасақтамасын қоса) осалдықтар туралы ақпарат және осалдықтарды түзету бағдарламалық жасақтамасының жаңартулары (Microsoft бағдарламалық жасақтамасын қоспағанда) Басқару серверіне жіберіледі.

  Осы параметрді таңдау (**Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер**) желі жүктемесін, Басқару сервері дискісінің жүктемесін және Желілік агент ресурстарын тұтынуды арттырады.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

  Microsoft бағдарламаларының жаңартуларын басқару үшін **Windows Update жаңартулар мәліметтері** параметрін пайдаланыңыз

- **Жабдық тізімдемесі туралы ақпарат**

  Құрылғыға орнатылған Желілік агент құрылғының жабдықтары туралы ақпаратты Басқару серверіне жібереді. Жабдық туралы ақпаратты құрылғының сипаттарынан көруге болады.

  lshw утилитасы, жабдық туралы ақпарат алғыңыз келетін Linux құрылғыларында орнатылғанын тексеріңіз. Виртуалды машиналардан алынған жабдық туралы мәлімет пайдаланылатын гипервизорға байланысты толық болмауы мүмкін

- **Орнатылған бағдарламалардың мәліметтері**

  Егер бұл параметр қосылса, клиент құрылғыларында орнатылған бағдарламалар туралы ақпарат Басқару серверге жіберіледі.

  Әдепкі бойынша, параметр қосулы.

- **Патчтар туралы ақпаратты қамту**

  Клиент құрылғыларында орнатылған бағдарлама патчтары туралы ақпарат Басқару серверіне жіберіледі. Бұл параметрді қосу, Басқару сервері мен ДҚБЖ-не түсетін жүктемені арттырып, дерекқор көлемінің ұлғаюына әкелуі мүмкін.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

Желілік агент саясатында, осы бөлімде көрсетілген параметрлерді өзгертуге тыйым салынса, бұл параметрлерді өзгерту мүмкін емес.

Бағдарламалық жасақтама жаңартулары мен осалдықтары

Бағдарламалық жасақтаманың жаңартулары мен осалдықтары бөлімінде Windows жаңартуларын іздеуді және таратуды конфигурациялауға, сондай-ақ орындалатын файлдарда осалдықтардың бар-жоғын сканерлеуді қосуға болады:

- **Басқару серверін WSUS сервері ретінде пайдалану**

  Егер бұл параметр қосулы болса, Windows жаңартулары Басқару серверіне жүктеледі. Басқару сервері жүктелген жаңартуларды Желілік агенттер арқылы клиент құрылғыларындағы Windows Update қызметтеріне орталықтан ұсынады.

  Егер бұл параметр өшірулі болса, Басқару сервері Windows жаңартуларын жүктеу үшін пайдаланылмайды. Бұл жағдайда, клиент құрылғылары Windows жаңартуларын өздері алады.

  Әдепкі бойынша, параметр өшірулі.

- **Пайдаланушыларға Windows Update жаңартуларын орнатуды басқаруға рұқсат беру** параметрі арқылы, пайдаланушылар Windows Update көмегімен өз құрылғыларына қолмен орната алатын Windows жаңартуларын шектей аласыз.

  Windows 10 операциялық жүйелері бар құрылғылар үшін, Windows Update-те құрылғыларға арналған жаңартулар табылса, онда сіз **Пайдаланушыларға Windows Update жаңартуларын орнатуды басқаруға рұқсат беру** астында таңдаған жаңа параметр, табылған жаңартуларды орнатқаннан кейін ғана қолданылады.

  Ашылмалы тізімнен параметрді таңдаңыз:

  - **Пайдаланушыларға барлық қолданылатын Windows Update жаңартуларын орнатуға рұқсат беру**

    Пайдаланушылар өз құрылғыларына қолданылатын барлық Windows Update жаңартуларын орната алады.

    Жаңартуларды орнатуға әсер еткіңіз келмесе, осы нұсқаны таңдаңыз.

    Пайдаланушы Windows Update жаңартуларын қолмен орнатқан кезде, жаңартуларды Басқару серверінен емес, Microsoft серверлерінен жүктеуге болады. Бұл, Басқару сервері бұл жаңартуларды әлі жүктемеген болса жүзеге асырылуы мүмкін. Microsoft серверлерінен жаңартуларды жүктеу трафиктің өсуіне әкеледі.

  - **Пайдаланушыларға тек расталған Windows Update жаңартуларын орнатуға рұқсат беру**

    Пайдаланушылар өз құрылғыларына қолданылатын және әкімші мақұлдаған барлық Windows Update жаңартуларын орната алады.

    Мысалы, сіз алдымен жаңартуларды сынақ ортасында орнатуды тексеріп, олар құрылғылардың жұмысына кедергі келтірмейтіндігіне көз жеткізіп алып, содан кейін осы мақұлданған жаңартуларды клиент құрылғыларына орнатуға рұқсат бере аласыз.

    Пайдаланушы Windows Update жаңартуларын қолмен орнатқан кезде, жаңартуларды Басқару серверінен емес, Microsoft серверлерінен жүктеуге болады. Бұл, Басқару сервері бұл жаңартуларды әлі жүктемеген болса жүзеге асырылуы мүмкін. Microsoft серверлерінен жаңартуларды жүктеу трафиктің өсуіне әкеледі.

  - **Пайдаланушыларға Windows Update жаңартуларын орнатуға рұқсат бермеу**

    Пайдаланушылар Windows Update жаңартуларын өз құрылғыларына қолмен орната алмайды. Барлық қолданылатын жаңартулар әкімші белгілеген конфигурацияға сәйкес орнатылады.

    Жаңартуларды орнатуды орталықтан басқарғыңыз келсе, осы нұсқаны таңдаңыз.

    Мысалы, желіні жүктемеу үшін жаңарту кестесін конфигурациялауға болады. Пайдаланушылардың өнімділігіне кедергі келтірмеу үшін жаңартуларды жұмыс уақытынан тыс жоспарлауға болады.

- **Windows Update жаңартуларын іздеу режимі** параметрлер блогында жаңартуларды іздеу режимін таңдауға болады:

  - **Белсенді**

    Егер бұл нұсқа таңдалса, Басқару сервері Желілік агенттің көмегімен клиент құрылғысындағы Windows жаңарту агентінің жаңарту көзіне: Windows Update Servers немесе WSUS серверіне жүгінуін бастайды. Содан соң, Желілік агент Windows Update агентінен алынған ақпаратты Басқару серверіне жібереді.

Бұл параметр, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы болса ғана қолданылады.

Әдепкі бойынша, осы нұсқа таңдалған.

- **Пассив**

  Егер бұл нұсқа таңдалса, Желілік агент Windows жаңарту агентін жаңарту көзімен соңғы рет синхрондау кезінде алынған жаңартулар туралы ақпаратты мезгіл-мезгіл Басқару серверіне жібереді. Windows жаңарту агентін жаңарту көзімен синхрондау орындалмаса, Басқару серверіндегі жаңартулар туралы деректер ескіреді.

  Жаңарту көзі кэшінен жаңартуларды алғыңыз келсе, осы параметрді таңдаңыз.

- **Өшірулі**

  Егер бұл нұсқа таңдалса, Басқару сервері жаңартулар туралы ақпаратты сұрамайды.

  Мысалы, алдымен жергілікті құрылғыдағы жаңартуларды тексергіңіз келсе, осы параметрді таңдаңыз.

- **Іске қосу кезінде орындалатын файлдарда осалдықтар бар-жоғын сканерлеу**

  Параметр қосулы болса, орындалатын файлдарды іске қосу кезінде олардың осалдығын тексеру жүргізіледі.

  Әдепкі бойынша, параметр қосулы.

Өшіріп қайта қосуды басқару

Қолданбаны дұрыс пайдалану, орнату не жою үшін басқарылатын құрылғының операциялық жүйесін өшіріп қосу қажет болса, **Өшіріп қайта қосуды басқару** бөлімінде орындалатын әрекетті көрсетуге болады.

- **Операциялық жүйені қайта жүктемеу**

  Операциялық жүйені қайта іске қосу орындалмайды.

- **Қажет болса, операциялық жүйені автоматты түрде қайта іске қосыңыз**

  Қажет болса, операциялық жүйені қайта іске қосу автоматты түрде орындалады.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Бағдарлама пайдаланушыдан операциялық жүйені қайта іске қосуға рұқсат сұрайды.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл параметр қосулы болса, бағдарлама пайдаланушыдан жалаушаның жанындағы өрісте көрсетілген жиілікпен операциялық жүйені қайта іске қосуға рұқсат сұрайды. Әдепкі бойынша, қайталанатын сұраулардың жиілігі 5 минутты құрайды.

    Егер бұл параметр өшірулі болса, бағдарлама қайта іске қосуға қайтадан рұқсат сұрамайды.

    Әдепкі бойынша, параметр қосулы.

  - **Осы уақыттан кейін мәжбүрлеп қайта іске қосу (мин)**

    Егер бұл параметр қосулы болса, пайдаланушыдан сұрау келіп түскеннен кейін, операциялық жүйе жалаушаның жанындағы өрісте көрсетілген уақыт өткеннен кейін қайта іске қосылады.

Осы параметр өшірулі болса, мәжбүрлеп қайта іске қосу орындалмайды.

Әдепкі бойынша, параметр қосулы.

- **Бұғатталған сессияларда бағдар. келесі уақыттан кейін мәжбүрлеп жабу (мин)**

  Пайдаланушының құрылғысы бұғатталған кезде бағдарламаларды мәжбүрлеп аяқтау (белсенді емес кезеңнен кейін автоматты түрде немесе қолмен).

  Егер параметр қосулы болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы енгізу өрісінде көрсетілген уақыт өткеннен кейін тоқтатылады.

  Егер параметр өшірулі болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы тоқтамайды.

  Әдепкі бойынша, параметр өшірулі.

Windows жұмыс үстелін бірлесіп пайдалану

Windows компьютерлік бөлісу қызметін пайдалану бөлімінде жұмыс үстелін бірлесіп пайдалану кезінде қашықтағы құрылғыда орындалатын әкімші әрекеттерінің аудитін қосуға және конфигурациялауға болады.

- **Аудитті қосу**

  Егер параметр қосулы болса, қашықтағы құрылғыдағы әкімші әрекетінің аудиті қосылады. Қашықтағы құрылғыдағы әкімші әрекеттері туралы жазбалар мында сақталады:

  - қашықтағы құрылғыдағы оқиғалар журналында;
  - қашықтағы құрылғыдағы Желілік агентті орнату қалтасында орналасқан syslog кеңейтімі бар файлда;
  - Kaspersky Security Center оқиғалар дерекқорында.

  Әкімші әрекеттерінің аудиті келесі шарттар орындалған кезде қолжетімді:

  - Осалдықтар мен патчтарды басқаруға арналған лицензия әлдеқашан қолданылады;
  - әкімшінің қашықтағы құрылғының жұмыс үстелін бірлесіп пайдалануға құқығы бар.

  Егер параметр өшірулі болса, қашықтағы құрылғыдағы әкімші әрекетінің аудиті өшіріледі.

  Әдепкі бойынша, параметр өшірулі.

- **Оқу кезінде бақыланатын файлдардың маскалары**

  Тізімде файл бүркеніштері сақталады. Аудит қосылған кезде, бағдарлама әкімшінің бүркеніштерге сәйкес келетін файлдарды оқуын қадағалайды және файлдарды оқу туралы ақпаратты сақтайды. **Аудитті қосу** жалаушасы қойылса, тізімді қолжетімді болады. Файл бүркеніштерін өзгертуге және тізімге жаңа бүркеніштер қосуға болады. Жаңа файл бүркеніштері тізімде жаңа жолдан көрсетілуі керек.

  Әдепкі бойынша *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf файлдарының бүркеніштері көрсетілген.

- **Өзгерткен кезде бақыланатын файлдардың маскалары**

  Тізімде қашықтағы құрылғыдағы файл бүркеніштері бар. Аудит қосылған кезде, бағдарлама әкімшінің бүркеніштерге сәйкес келетін файлдарды өзгертуін қадағалайды және файлдарды өзгерту туралы ақпаратты сақтайды. **Аудитті қосу** жалаушасы қойылса, тізімді қолжетімді болады. Файл бүркеніштерін өзгертуге және тізімге жаңа бүркеніштер қосуға болады. Жаңа файл бүркеніштері тізімде жаңа жолдан көрсетілуі керек.

  Әдепкі бойынша *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf файлдарының бүркеніштері көрсетілген.

Патчтарды және жаңартуларды басқару

Патчтарды және жаңартуларды басқару бөлімінде жаңартуларды алу мен таратуды және патчтарды басқарылатын құрылғыларға орнатуды конфигурациялауға болады:

- **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату**

  Егер жалауша қойылса, *Анықталмаған* мақұлдау мәртебесі бар Kaspersky патчтары жаңарту серверлерінен жүктелгеннен кейін автоматты түрде басқарылатын құрылғыларға орнатылады.

  Егер жалауша алынып тасталса, *Анықталмаған* мәртебесі бар Kaspersky жүктелген патчтары, әкімші олардың мәртебесін *Расталды* деп өзгерткеннен кейін орнатылады.

  Әдепкі бойынша, параметр қосулы.

- **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)**

  Параметр қосулы болса, жаңартуларды алуға арналған офлайн-модель қолданылады. Басқару сервері жаңартуларды алған кезде, ол Желілік агентті (ол орнатылған құрылғыларда) басқарылатын бағдарламалар үшін қажет етілетін жаңартулар туралы хабардар етеді. Желілік агенттер жаңартулар туралы ақпаратты алған кезде, олар Басқару серверінен қажетті файлдарды ертерек жүктеп алады. Бірінші рет қосылған кезде, Сервер осы Агенттің жаңартуларды жүктеуіне түрткі болады. Желілік агент клиент құрылғысында барлық жаңартуларды жүктегеннен кейін, жаңартулар құрылғыдағы бағдарламалар үшін қолжетімді болады.

  Клиент құрылғысындағы басқарылатын бағдарлама жаңартуларды алу үшін Желілік агентке жүгінген кезде, Агент өзінде қажетті жаңартулардың бар ма екенін тексереді. Жаңартулар басқарылатын бағдарлама сұрау салған сәттен бастап 25 сағаттан ерте болмайтын мерзімнің ішінде Басқару серверінен алынған болса, онда Желілік агент Басқару серверіне қосылмайды және басқарылатын бағдарламаға жергілікті кэштегі жаңартуларды ұсынады. Желілік агент бағдарламаларға арналған жаңартуларды клиент құрылғыларында ұсынса, бірақ жаңарту үшін қосылым талап етілмесе, Басқару серверімен қосылым орындалмауы мүмкін.

  Параметр өшірулі болса, жаңартуларды жүктеп алудың офлайн үлгісі пайдаланылмайды. Жаңартулар, жаңартуларды жүктеу тапсырмасының кестесіне сәйкес таратылады.

  Әдепкі бойынша, параметр қосулы.

Қосылымдар

Қосылым мүмкіндігі бөлімі үш ішкі бөлімді қамтиды:

- **Желі**
- **Байланыс профильдері** (тек Windows және macOS үшін)
- **Байланыс кестесі**

Желі бөлімінде Басқару серверіне қосылым параметрлерін конфигурациялауға, UDP портын пайдалану мүмкіндігін қосуға және оның нөмірін көрсетуге болады. Келесі параметрлер қолжетімді:

- **Басқару серверіне қосылу** блогында Басқару серверіне қосылу параметрлерін конфигурациялауға және клиент құрылғыларының Басқару серверімен синхрондау кезеңін көрсетуге болады:

  - **Желілік трафикті қысу**

    Егер параметр өшірулі болса, Желілік агент деректерін беру жылдамдығы арттырылады, берілетін ақпарат көлемі азайтылады және Басқару серверіне түсетін жүктемені азайтады.

    > Клиент компьютерінің орталық процессорына түсетін жүктеме артуы мүмкін.

    Әдепкі бойынша, жалауша қойылған.

  - **Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу**

    Параметр қосылса, Желілік агенттің жұмысына қажетті порттар Microsoft Windows брандмауэрінің ерекшеліктер тізіміне қосылады.

    Әдепкі бойынша, параметр қосулы.

  - **SSL пайдалану**

    Бұл параметр қосулы болса, Басқару серверіне қосылу SSL протоколының көмегімен, қорғалған порт арқылы орындалатын болады.

    Әдепкі бойынша, параметр қосулы.

  - **Әдепкі байланыс параметрлері астындағы тарату нүктесіндегі (қолжетімді болса) байланыс шлюзін пайдаланыңыз**

    Егер параметр қосулы болса, онда параметрлері басқару тобының сипаттарында белгіленген тарату нүктесінің қосылым шлюзі қолданылады.

    Әдепкі бойынша, параметр қосулы.

- **UDP портын пайдалану**

  Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

- **UDP портының нөмірі**

  Өрісте UDP портының нөмірін енгізуге болады. Әдепкі бойынша 15000-порт орнатылған.

  Ондық жазба нысаны қолданылады.

  Егер клиент құрылғысы Windows XP Service Pack 2 операциялық жүйесінің басқаруымен жұмыс істесе, кірістірілген желілік экран 15000 нөмірі бар UDP портын бұғаттайды. Бұл портты қолмен ашу керек.

- **Басқару серверіне мәжбүрлі қосылу үшін тарату нүктесін пайдаланыңыз**

  Егер сіз тарату нүктесі опциялары терезесінде **Осы тарату нүктесін push сервері ретінде пайдалану** параметрін таңдасаңыз, осы параметрді таңдаңыз. Әйтпесе, тарату нүктесі push серверінің рөлін атқармайды.

Байланыс профильдері бөлімінде желілік орналасқан жер параметрлерін белгілеуге, Басқару серверіне қосылу профильдерін конфигурациялауға, Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысуға болады.

- **Желілік орналасудың параметрлері**

  Желілік орналасудың параметрлері клиент құрылғысы қосылған желінің сипаттамаларын анықтайды және желі сипаттамалары өзгерген кезде Желілік агентті бір Басқару сервері қосылымы профилінен екіншісіне ауыстыру ережелерін белгілейді.

- **Басқару серверіне қосылу профильдері**

  Бұл бөлімде Желілік агенттің Басқару серверіне қосылу профильдерін қарауға және қосуға болады. Бұл бөлімде келесі оқиғалар орын алған кезде Желілік агентті басқа Басқару серверіне ауыстыру ережелерін құрастыруға болады:

  - клиент құрылғысын басқа жергілікті желіге қосу;
  - құрылғыны ұйымның жергілікті желісінен ажырату;
  - қосылым шлюзінің мекенжайын өзгерту немесе DNS серверінің мекенжайын өзгерту.

  Қосылым профильдеріне тек Windows және macOS басқаратын құрылғылар үшін ғана қолдау көрсетіледі.

- **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу**

  Параметр қосулы болса, осы профиль арқылы қосылу кезінде, клиент бағдарламасында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясат профильдерін және автономды пайдаланушыларға арналған саясаттарды қолданатын болады. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, бағдарламалар белсенді саясаттарды қолданатын болады.

  Әдепкі бойынша, параметр өшірулі.

Байланыс кестесі бөлімінде Желілік агент деректерді Басқару серверіне жіберетін уақыт аралықтарын белгілеуге болады:

- **Қажет болғанда қосылу**

  Егер бұл нұсқа таңдалса, байланыс Желілік агент деректерді Басқару серверіне жіберуі қажет болған кезде орнатылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Көрсетілген кезеңдерде қосылу**

  Егер бұл нұсқа таңдалса, Желілік агентті Басқару серверіне қосу белгілі бір уақыт аралығында жүзеге асырылады. Бірнеше қосылу кезеңдерін қосуға болады.

Тарату нүктелері

Тарату нүктелері бөлімі төрт ішкі бөлімді қамтиды:

- **Желі сауалнамалары**
- **Интернетке қосылу параметрлері**
- **KSN Проксиі**
- **Жаңартулар**

Желі сауалнамалары бөлікшесінде автоматты желі сауалнамаларын конфигурациялауға болады. Сіз сауалнаманың үш түрін, яғни желі сауалнамасын, IP ауқымдарының сауалнамасын және Active Directory сауалнамасын қоса аласыз:

- **Желі сауалнамасына рұқсат ету**

  Егер бұл параметр қосылса, Басқару сервері **Жылдам сауалнама жүргізу кестесін орнату** және **Толық сауалнама жүргізу кестесін орнату** сілтемелері бойынша конфигурацияланған кестеге сәйкес желіге автоматты түрде сауалнама жүргізеді.

  Бұл параметр өшірілсе, Басқару сервері **Желі сұрауларының жиілігі (мин)** өрісінде көрсетілген кезеңмен желіде сауалнама өткізеді.

  10.2-ден төмен басқару серверіне арналған құрылғыларды анықтау уақытын **Windows домендерінен сұраулар жиілігі (мин)** (Windows желісінде жылдам сұрау жүргізу үшін) және **Желі сұрауларының жиілігі (мин)** (Windows желісінде толық сұрау жүргізу үшін) өрістерінде реттеуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **IP ауқымы бойынша сауалнама өткізуді қосу**

  Егер бұл параметр қосылса, тарату нүктесі **Сауалнама кестесін орнату** түймесі бойынша конфигурацияланған кестеге сәйкес IP ауқымына автоматты түрде сауалнама жүргізеді.

  Егер параметр өшірулі болса, тарату нүктесі IP ауқымдарының сауалнамасын өткізеді.

  10.2-ден төмен нұсқаны Желілік агент нұсқалары үшін IP ауқымдарының сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде конфигурациялауға болады. Егер параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

- **Zeroconf сауалнамасын қолданыңыз (тек Linux платформаларында; қолмен көрсетілген IP ауқымдары еленбейді)**

  Егер бұл параметр қосулы болса, тарату нүктесі автоматты түрде нөлдік конфигурациясы бар желіні (бұдан әрі *Zeroconf*) пайдалану арқылы IPv6 құрылғылары бар желіде автоматты түрде сауалнама өткізеді. Бұл жағдайда, IP ауқымдарының сауалнамасы еленбейді, өйткені тарату нүктесі бүкіл желіге сауалнама жүргізеді.

  Zeroconf пайдалануды бастау үшін келесі шарттар орындалуы керек:

  - Тарату нүктесі Linux басқаруымен жұмыс істеуі керек.
  - Тарату нүктесіне avahi-browse утилитасын орнату қажет.

  Егер бұл параметр өшірілген болса, тарату нүктесі IPv6 құрылғылары бар желілерде сауалнама жүргізбейді.

  Әдепкі бойынша, параметр өшірулі.

- **Active Directory сауалнамасын қосу**

  Егер бұл параметр қосылса, тарату нүктесі **Сауалнама кестесін орнату** сілтемесі бойынша конфигурацияланған кестеге сәйкес Active Directory сауалнамасын жүргізеді.

  Егер параметр өшірулі болса, Басқару сервері Active Directory сауалнамасын жүргізбейді.

  10.2-ден төмен нұсқаны Желілік агент нұсқалары үшін Active Directory сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде конфигурациялауға болады. Егер осы параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

Егер тарату нүктелері интернетке қосылған кезде прокси-серверді пайдаланса, **Интернетке қосылу параметрлері** ішкі бөлімінде келесі параметрлерді көрсетуге болады:

- **Прокси-серверді пайдалану**

  Егер бұл құсбелгі таңдалса, тарату нүктелерін Kaspersky жаңарту серверлеріне қосу үшін Интернет прокси-сервері пайдаланылады. Енгізу өрістерінде прокси-серверге қосылу параметрлерін баптауға болады.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Прокси-сервердің мекенжайы**

  Прокси серверінің мекенжайы.

- **Порт нөмірі**

  Қосылым орындалатын порт нөмірі.

- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Егер параметр қосулы болса, жергілікті желідегі құрылғыларға қосылған кезде прокси сервері пайдаланылмайды.

  Әдепкі бойынша, параметр өшірулі.

- **Прокси-сервердегі түпнұсқалық растама**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Пайдаланушы аты**

  Прокси-серверге қосылу орындалатын реттелетін есептік жазбасы.

- **Құпиясөз**

  Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

KSN Проксиі бөлімінде бағдарламаны тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын жіберу үшін пайдаланылатындай етіп орнатуға болады:

- **Тарату нүктесі тарапынан KSN проксиін қосу**

  KSN прокси-сервері қызметі тарату нүктесі ретінде әрекет ететін құрылғыда орындалады. Бұл параметрді желі трафигін қайта тарату және оңтайландыру үшін пайдаланыңыз.

  Тарату нүктесі Kaspersky Security Network мәлімдемесінде көрсетілген KSN статистикасын Kaspersky ұйымына жібереді.

Әдепкі бойынша, параметр өшірулі. Осы параметрді қосу, **Басқару серверін прокси-сервер ретінде пайдалану** және **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрлері Басқару серверінің сипаттары терезесінде қосылған жағдайда ғана күшіне енеді.

Суық резерві бар істен шығуға төзімді кластер түйініне (белсенді / пассивті) тарату нүктесін тағайындауға және сол түйінде KSN прокси-серверін қосуға болады.

- **KSN сұрауын Басқару серверіне қайта жіберу**

  Тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын Басқару серверіне жібереді.

  Әдепкі бойынша, параметр қосулы.

- **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру**

  Тарату нүктесі KSN-ге басқарылатын құрылғылардан KSN немесе KPSN бұлттық қызметіне сұраулар жібереді. Тарату нүктесінде жасалған KSN сұраулары да тікелей KSN Cloud немесе KPSN-ге жіберіледі.

  Желілік агенттің 11 (немесе одан бұрынғы) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алмайды. Тарату нүктелерін KSN сұрауларын KSN-ге жіберу үшін қайта реттегіңіз келсе, әрбір тарату нүктесі үшін **KSN сұрауын Басқару серверіне қайта жіберу** параметрін қосыңыз.

  Желілік агенттің 12 (және одан да жоғары) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алады.

- **TCP порты**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын TCP портының нөмірі. Әдепкі бойынша 13111-порт орнатылған.

- **UDP портын пайдалану**

  Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

Жаңартулар ішкі бөлімінде **diff файлдарды жүктеп алу** опциясын қосу не өшіру арқылы желілік агенттің diff файлдарын жүктеп алуы қажет пе екенін көрсетуге болады. (Әдепкісінше бұл опция қосылады.)

Тексерістер журналы

Тексерістер журналы қойыншасында Желілік агенттің тексерістер журналын қарап шығуға болады. Сіз тексерулерді салыстыра аласыз, тексерулерді қарап шыға аласыз және тексерулерді файлға сақтау, тексерулерді қайтарып алу, тексеру сипаттамаларын қосу және өзгерту сияқты басқа да операцияларды орындай аласыз.

Пайдаланушы есептік жазбаларын басқару

Бұл бөлімде бағдарлама қолдайтын есептік жазбалар мен пайдаланушы рөлдері туралы ақпарат бар. Бөлімде Kaspersky Security Center пайдаланушыларының есептік жазбалары мен рөлдерін жасау бойынша нұсқаулар берілген.

Kaspersky Security Center пайдаланушы есептік жазбалары мен есептік жазбалар топтарын басқаруға мүмкіндік береді. Қолданба есептік жазбалардың үш түрін қолдайды:

- Ұйым қызметкерлерінің есептік жазбалары. Басқару сервері ұйымның домен контроллерінде сауалнама жүргізу кезінде осы домен пайдаланушыларының есептік жазбалары туралы деректерді алады.
- Жергілікті пайдаланушылардың есептік жазбалары. Басқарылатын құрылғылардың жергілікті есептік жазбалары, сондай-ақ басқару сервері орнатылған құрылғының жергілікті есептік жазбалары.
- Kaspersky Security Center ішкі пайдаланушыларының есептік жазбалары. Ішкі пайдаланушылардың есептік жазбаларын жасай аласыз. Бұл есептік жазбалар тек Kaspersky Security Center жүйесінде пайдаланылады.

Пайдаланушы есептік жазбаларымен жұмыс

Kaspersky Security Center пайдаланушы есептік жазбалары мен есептік жазбалар топтарын басқаруға мүмкіндік береді. Бағдарлама есептік жазбалардың екі түрін қолдайды:

- Ұйым қызметкерлерінің есептік жазбалары. Басқару сервері ұйымның желісінде сауалнама жүргізу кезінде осы пайдаланушылардың есептік жазбалары туралы мәліметтерді алады.
- Ішкі пайдаланушылардың есептік жазбалары. Виртуалды Басқару серверлерімен жұмыс істеу үшін қолданылады. Ішкі пайдаланушы есептік жазбалары тек Kaspersky Security Center ішінде жасалады және пайдаланылады.

Пайдаланушы есептік жазбаларының тізімін келесі жолдардың бірімен көре аласыз:

- Консоль тармағында **Кеңейтілген** → **Пайдаланушылардың есептік жазбалары** тармағына өтіңіз.
- Консоль тармағында **Басқарылатын құрылғылар** қалтасына → **Құрылғылар** қойындысына → <құрылғы атауы> сілтемесіне → **Сеанстар** бөліміне өтіңіз.

  Сеанстар бөлімінде Windows басқаратын құрылғыларда белсенді сеанстары бар пайдаланушылар есептік жазбалары көрсетіледі.

Келесі талаптар орындалса, пайдаланушы есептік жазбаларының тізімі дұрыс шығады:

- Нұсқасы басқару серверінің нұсқасымен бірдей немесе одан жоғары желілік агент қолданылып жатыр.
- Active Directory сұрауы домен пайдаланушыларының есептік жазбаларын көрсету үшін қосылған.
- Windows басқаратын құрылғыларда **Сервер қызметі (LanmanServer)** жұмыс істейді.

Пайдаланушы есептік жазбаларымен және есептік жазбалар топтарымен келесі әрекеттерді орындауға болады:

- пайдаланушылардың рөлдер арқылы бағдарлама функцияларына қатынасу құқықтарын конфигурациялау;
- электрондық пошта және SMS арқылы пайдаланушыларға хабар жіберу;
- пайдаланушының ұялы құрылғыларының тізімін қарау;
- пайдаланушының ұялы құрылғыларына сертификаттар жазып беру және орнату;

- пайдаланушыға берілген сертификаттар тізімін қарап шығу;
- пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру.

Ішкі пайдаланушының есептік жазбасын қосу

Kaspersky Security Center жаңа пайдаланушы есептік жазбасын қосу үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын ашыңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Жұмыс аймағында **Пайдаланушыны қосу** түймесін басыңыз.

3. Ашылған **Жаңа пайдаланушы** терезесінде жаңа пайдаланушы параметрлерін көрсетіңіз:

   - Пайдаланушы аты (👨).

     > Пайдаланушы атын енгізген кезде абай болыңыз. Өзгерістерді сақтағаннан кейін оны өзгерте алмайсыз.

   - **Сипаттама**
   - **Толық атауы**
   - **Негізгі электрондық пошта**
   - **Негізгі телефон нөмірі**
   - Пайдаланушыны Kaspersky Security Center-ге қосуға арналған **Құпиясөз**.

     Құпиясөз келесі ережелерге сәйкес келуі керек:

     - Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
     - Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
       - Бас әріптер (A-Z)
       - Кіші әріптер (a-z)
       - Сандар (0-9)
       - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

     Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Пайдаланушының құпиясөз енгізу әрекеттерінің саны шектеулі. Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Енгізу әрекеттерінің максималды санын "Құпиясөз енгізу әрекеттерінің санын енгізу" бөлімінде сипатталғандай, өзгертуге болады.

Егер пайдаланушы құпиясөзді бірнеше рет қате енгізсе, пайдаланушы есептік жазбасы бір сағатқа бұғатталады. Пайдаланушы есептік жазбалары тізімінде бұғатталған есептік жазбаның белгішесі қараңғыланған (қолжетімді емес). Сіз есептік жазбаны тек құпиясөзді ауыстыру арқылы бұғаттан босата аласыз.

- Қажет болса, пайдаланушының бағдарламаға қосылуына жол бермеу үшін **Есептік жазбаны өшіру** жалаушасын қойыңыз. Мысалы, есептік жазбаны алдын ала жасағыңыз келсе, бірақ оны кейінірек іске қосқыңыз келсе, есептік жазбаны өшіруге болады.

- Пайдаланушы есептік жазбасын рұқсатсыз өзгертуден қосымша қорғанысты қосқыңыз келсе, **Есептік жазба параметрлері өзгертілген кезде құпиясөз сұраңыз** жалаушасын қойыңыз. Осы параметр қосулы болса, онда пайдаланушы есептік жазбасының параметрлерін өзгерту үшін **Жалпы функционал: Пайдаланушы рұқсаттары** аймағындағы Нысан ACL параметрлерін өзгерту құқығы бар пайдаланушының авторизациясы қажет.

4. **OK** түймесін басыңыз.

Жасалған пайдаланушы есептік жазбасы **Пайдаланушылардың есептік жазбалары** қалтасының жұмыс аймағында көрсетіледі.

Ішкі пайдаланушының есептік жазбасын өзгерту

Kaspersky Security Center ішкі пайдаланушы есептік жазбасын өзгерту үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын ашыңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Жұмыс аймағында өзгертуді қажет ететін ішкі пайдаланушы есептік жазбасын екі рет басыңыз.

3. Ашылған **Сипаттар: <пайдаланушы атауы>** терезесінде пайдаланушы есептік жазбасының параметрлерін өзгертіңіз:

   - **Сипаттама**
   - **Толық атауы**
   - **Негізгі электрондық пошта**
   - **Негізгі телефон нөмірі**
   - Пайдаланушыны Kaspersky Security Center-ге қосуға арналған **Құпиясөз**.

Құпиясөз келесі ережелерге сәйкес келуі керек:

- Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Пайдаланушының құпиясөз енгізу әрекеттерінің саны шектеулі. Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Енгізу әрекеттерінің максималды санын "Құпиясөз енгізу әрекеттерінің санын енгізу" бөлімінде сипатталғандай, өзгертуге болады.

Егер пайдаланушы құпиясөзді бірнеше рет қате енгізсе, пайдаланушы есептік жазбасы бір сағатқа бұғатталады. Пайдаланушы есептік жазбалары тізімінде бұғатталған есептік жазбаның белгішесі қараңғыланған (қолжетімді емес). Сіз есептік жазбаны тек құпиясөзді ауыстыру арқылы бұғаттан босата аласыз.

- Қажет болса, пайдаланушының бағдарламаға қосылуына жол бермеу үшін **Есептік жазбаны өшіру** жалаушасын қойыңыз. Мысалы, қызметкер компаниядан жұмыстан шыққаннан кейін, есептік жазбаны өшіруге болады.
- Пайдаланушы есептік жазбасын рұқсатсыз өзгертуден қосымша қорғанысты қосқыңыз келсе, **Есептік жазба параметрлері өзгертілген кезде құпиясөз сұраңыз** параметрін таңдаңыз. Осы параметр қосулы болса, онда пайдаланушы есептік жазбасының параметрлерін өзгерту үшін **Жалпы функционал: Пайдаланушы рұқсаттары** аймағындағы Нысан ACL параметрлерін өзгерту құқығы бар пайдаланушының авторизациясы қажет.

4. **OK** түймесін басыңыз.

Өзгертілген пайдаланушы есептік жазбасы **Пайдаланушылардың есептік жазбалары** қалтасының жұмыс аймағында көрсетіледі.

Құпиясөзді енгізу әрекеттерінің санын өзгерту

Kaspersky Security Center пайдаланушысы құпиясөзді шектеулі рет енгізе алады. Осыдан кейін, пайдаланушы есептік жазбасы бір сағатқа бұғатталады.

Әдепкі бойынша, енгізу әрекеттерінің максималды саны 10-ға тең. Төмендегі нұсқауларды орындау арқылы құпиясөзді енгізу әрекеттерінің санын өзгертуге болады.

Құпиясөзді енгізу әрекеттерінің санын өзгерту үшін келесі әрекеттерді орындаңыз:

1. Басқару сервері орнатылған құрылғының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.
2. Келесі бөлімге өтіңіз:
   - 32 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 64 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. SrvSplPpcLogonAttempts параметрі тізімдеме бөлімінде болмаса, оны жасаңыз. Параметр мәнінің түрі – DWORD.

   Бұл параметр Kaspersky Security Center орнату кезінде әдепкі бойынша жасалмайды.
4. SrvSplPpcLogonAttempts параметрінің мәні ретінде қажетті әрекеттер санын көрсетіңіз.
5. Өзгерістерді сақтау үшін **OK** түймесін басыңыз.
6. Басқару сервері қызметін қайта іске қосыңыз.

Құпиясөзді енгізу әрекеттерінің максималды саны өзгертілді.

Ішкі пайдаланушы атының бірегейлігін тексеруді конфигурациялау

Kaspersky Security Center ішкі пайдаланушысы атын бағдарламаға қосқан кезде, оның бірегейлігін тексеруді конфигурациялауыңызға болады. Ішкі пайдаланушы атының бірегейлігін тексеру тек виртуалды Серверде немесе пайдаланушы есептік жазбасы жасалатын басты Серверде немесе барлық виртуалды Серверлерде және басты Серверде ғана орындалуы мүмкін. Әдепкі бойынша, ішкі пайдаланушы атының бірегейлігін тексеру барлық виртуалды Серверлерде және басты Басқару серверінде орындалады.

Виртуалды Сервер немесе басты Сервер шеңберінде ішкі пайдаланушы атының бірегейлігін тексеруді қосу үшін:

1. Басқару сервері орнатылған құрылғының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.
2. Келесі бөлімге өтіңіз:
   - 32 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 64 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. LP_InterUserUniqVsScope (DWORD) кілтіне 00000001 мәнін белгілеңіз.

   Әдепкі бойынша, бұл кілт үшін 0 мәні көрсетілген.

4. Басқару сервері қызметін қайта іске қосыңыз.

Нәтижесінде, аттың бірегейлігін тексеру тек ішкі пайдаланушы жасалған виртуалды Серверде немесе пайдаланушы басты Серверде жасалған болса — басты Серверде орындалады.

Барлық виртуалды Серверлерде және басты Серверде ішкі пайдаланушы атының бірегейлігін тексеруді қосу үшін:

1. Басқару сервері орнатылған құрылғының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.

2. Келесі бөлімге өтіңіз:

   - 64 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - 32 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. LP_InterUserUniqVsScope (DWORD) кілтіне 00000000 мәнін белгілеңіз.

   Әдепкі бойынша, бұл кілт үшін 0 мәні көрсетілген.

4. Басқару сервері қызметін қайта іске қосыңыз.

Нәтижесінде, аттың бірегейлігін тексеру барлық виртуалды Серверлерде және басты Басқару серверінде орындалады.

Қауіпсіздік топтарын қосу

Қауіпсіздік топтарын (пайдаланушы топтарын) қосуға, топтар құрамын және қауіпсіздік тобының бағдарламаның әртүрлі функцияларына қатынасуын икемді түрде конфигурациялауға болады. Қауіпсіздік топтарына олардың мақсатына сәйкес атаулар берілуі мүмкін. Мысалы, атау кеңседегі пайдаланушылардың орналасқан жеріне немесе пайдаланушылар қатысты болып табылатын компанияның құрылымдық бөлімшесінің атауына сәйкес келуі мүмкін.

Бір пайдаланушы бірнеше қауіпсіздік топтарының құрамына кіруі мүмкін. Виртуалды Басқару сервері басқаратын пайдаланушы есептік жазбасы тек осы виртуалды Сервердің қауіпсіздік топтарына кіре алады және тек осы виртуалды Сервер шеңберінде қатынасу құқықтарына ие бола алады.

Қауіпсіздік тобын қосу үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. **Қауіпсіздік тобын қосу** түймесін басыңыз.

   Қауіпсіздік тобын қосу терезесі ашылады.

3. **Қауіпсіздік тобын қосу** терезесінде, **Жалпы** бөлімінде топтың атауын көрсетіңіз.

Топтың атауы 255 таңбадан асуы және *, <, >, ?, \, :, | таңбаларын қамтуы мүмкін емес. Топтың атауы бірегей болуы керек.

Топ сипаттамасын **Сипаттама** енгізу өрісінде енгізе аласыз. **Сипаттама** өрісін толтыру міндетті емес.

4. **ОК** түймесін басыңыз.

Қосылған қауіпсіздік тобы консоль ағашындағы **Пайдаланушылардың есептік жазбалары** қалтасында көрсетіледі. Сіз пайдаланушыларды жасалған топқа қоса аласыз.

Пайдаланушыны топқа қосу

Пайдаланушыны топқа қосу үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Пайдаланушы және топтар есептік жазбаларының тізімінен пайдаланушы қосылуы қажет топты таңдаңыз.

3. Топ сипаттары терезесінде **Топ пайдаланушылары** бөлімін таңдап, **Қосылуда** түймесін басыңыз.

   Нәтижесінде, пайдаланушылар тізімі бар терезе ашылады.

4. Тізімде топтың құрамына қосылатын пайдаланушыны немесе пайдаланушыларды таңдаңыз.

5. **ОК** түймесін басыңыз.

Пайдаланушы топқа қосылады және топ пайдаланушыларының тізімінде көрсетіледі.

Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау. Рөлге негізделген қатынасуды басқару

Kaspersky Security Center бағдарламасы рөлдер негізінде Kaspersky Security Center функцияларына және Kaspersky басқарылатын бағдарламаларының функцияларына қатынасуды қамтамасыз етеді.

Сіз Kaspersky Security Center пайдаланушылары үшін бағдарлама функцияларына қатынасу құқығын келесі тәсілдердің бірімен конфигурациялай аласыз:

- әр пайдаланушының немесе пайдаланушылар тобының құқықтарын жеке-жеке конфигурациялау;
- алдын ала конфигурацияланған құқықтар жиынтығы бар типтік пайдаланушы рөлдерін жасау және пайдаланушыларға олардың қызметтік міндеттеріне қарай рөлдер тағайындау.

Пайдаланушы рөлі (бұдан әрі - рөл) – бұл Kaspersky Security Center функцияларына немесе Kaspersky басқарылатын бағдарламаларына қатынасу құқықтарының алдын ала анықталған жиынтығы. Рөлді пайдаланушыға немесе пайдаланушылар тобына тағайындауға болады.

Пайдаланушы рөлдерін қолдану пайдаланушының бағдарламаға қатынасу құқығын конфигурациялаудың күнделікті әрекеттерін жеңілдетеді және азайтады. Рөлдегі қатынасу құқықтары пайдаланушылардың типтік тапсырмалары мен қызметтік міндеттеріне сәйкес конфигурацияланады.

Пайдаланушы рөлдеріне олардың мақсатына сәйкес атаулар берілуі мүмкін. Бағдарламада рөлдердің шексіз санын жасай аласыз.

Сіз алдын ала анықталған пайдаланушы рөлдерін бұрыннан конфигурацияланған құқықтар жиынтығымен бірге пайдалана аласыз немесе рөлдер жасай аласыз және қажетті құқықтарды өзіңіз конфигурациялай аласыз.

Бағдарлама функцияларына қатынасу құқықтары

Төмендегі кестеде тапсырмаларды, есептерді, параметрлерді басқаруға және пайдаланушы әрекеттерін орындауға құқық беретін Kaspersky Security Center функциялары берілген.

Кестеде көрсетілген пайдаланушы әрекеттерін орындау үшін пайдаланушының әрекеттің жанында көрсетілген құқығы болуы керек.

Оқу, **Жазу** және **Орындау** құқықтары кез келген тапсырмаға, есепке немесе параметрге қолданылады. Осы құқықтармен қоса, құрылғы таңдауларында тапсырмаларды, есептерді немесе параметрлерді басқару үшін пайдаланушыда **Құрылғылардың таңдауларында әрекеттерді орындау** құқығы болуы керек.

Кестеде жоқ барлық тапсырма, есеп, параметр және орнату пакеті **Жалпы функционал: Базалық функционалдылық** функционалдық аймағына жатады.

Бағдарлама функцияларына қатынасу құқықтары

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функционал: Басқару топтарын басқару	**Жазу**	• Құрылғыны басқару тобына қосу: **Жазу** • Басқару тобынан құрылғыны жою: **Жазу** • Басқа басқару тобына басқару қосутобын қосыңыз: **Жазу** • Басқа басқару тобынан басқару тобын жою: **Жазу**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функционал: ACL тізіміне қарамастан, нысандарға қатынасу	**Оқу**	Барлық нысанға Оқу рұқсат алу: **Оқу**	Жоқ	Жоқ	Жоқ
Жалпы функционал: Базалық функционалдылық	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Виртуалды серверге арналған құрылғыны жылжыту ережелері (жасау, өзгерту немесе жою): **Жазу**, **Құрылғылардың таңдауларында әрекеттерді орындау** • Мобильдік (LWNGT) протоколдың арнаулы сертификатын алу: **Оқу** • Мобильдік (LWNGT) протоколдың арнаулы сертификатын орнату: **Жазу** • NLA анықталған желі тізімін алу: **Оқу** • NLA анықталған желі тізімін қосу, өзгерту немесе жою: **Жазу** • Көру рұқсатын басқару топтарының тізімі: **Оқу** • Kaspersky оқиғалар журналын көру: **Оқу** • BitLocker арқылы шифрланған қатқыл дискіге кіруді қалпына келтіру үшін қалпына келтіру кілтін көру: **Орындау**	• "Жаңартуларды Басқару серверінің қоймасына жүктеп алу" • "Есептерді жеткізу" • "Орнату пакеттерін тарату" • "Қосалқы Басқару серверлеріне бағдарламаларды орнату"	• "Қорғаныс жағдайы туралы есеп" • "Қауіп-қатер туралы есеп" • "Ең көп зақымдалған құрылғылар туралы есеп" • "Антивирустық дерекқордың күйі туралы есеп" • "Қателер туралы есеп" • "Желілік шабуылдар туралы есеп" • "Пошталық жүйелерді қорғауға арналған бағдарламалар туралы жиынтық есеп" • "Периметрді қорғайтын бағдарламалар туралы жиынтық есеп" • "Орнатылған бағдарлама түрлері туралы жиынтық есеп" • "Вирус жұққан құрылғылардың пайдаланушылары туралы есеп" • "Инциденттер туралы есеп" • "Оқиғалар туралы есеп" • "Тарату нүктелерінің әрекетіндегі есеп" • "Қосалқы Басқару серверлері туралы есеп" • "Құрылғыларды басқару оқиғалары туралы есеп" • "Осалдықтар туралы есеп" • "Рұқсат берілмеген бағдарламалар бойынша есеп" • "Веб-бақылау туралы есеп" • "Басқарылатын құрылғыларды шифрлаудың күйі туралы есеп" • "Жаппай сақтау құрылғыларын шифрлау күйі туралы есепті көру"	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
				• "Файлдарды шифрлау қателері туралы есеп" • "Шифрланған файлдарға қатынасты бұғаттау туралы есеп" • "Шифрланған құрылғыларға қатынасу құқықтары туралы есеп" • "Пайдаланушының тиімді құқықтары туралы есеп" • "Құқықтар туралы есеп"	
Жалпы функционал: Жойылған нысандар	• **Оқу** • **Жазу**	• Себеттегі жойылған нысандарды көру: **Оқу** • Себеттен нысандарды жою: **Жазу**	Жоқ	Жоқ	Жоқ
Жалпы функционал: Оқиғаларды өңдеу	• **Оқиғалар жойылуда** • **Оқиғаның хабарландыру параметрлерін өңдеу** • **Оқиғаларды тіркеу параметрлерін өңдеу** • **Жазу**	• Оқиғаларды тіркеу параметрлерін өзгерту: **Оқиғаларды тіркеу параметрлерін өңдеу** • Оқиғалар туралы хабарландыру параметрлерін өзгерту: **Оқиғаның хабарландыру параметрлерін өңдеу** • Оқиғаларды жою: **Оқиғалар жойылуда**	Жоқ	Жоқ	Параметр • Виру шабу пара виру шабу оқиға жаса қаже виру анық • Виру шабу пара виру анық бағал • Дере сақта оқиға макс саны • Қашы құры оқиға сақта
Жалпы функционал: Басқару серверіне қатысты әрекеттер	• **Оқу** • **Жазу** • **Орындау** • **Нысан ACL параметрлерін өзгерту** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Желілік агент қосылымы үшін басқару серверінің порттарын көрсету: **Жазу** • Басқару серверінде іске қосылған белсендіру прокси порттарын көрсету: **Жазу** • Басқару серверінде іске қосылған мобильдік телефонға арналған белсендіру прокси порттарын көрсету: **Жазу**	• "Басқару сервері деректерінің сақтық көшірмесін жасау" • "Дерекқорларға қызмет көрсету"	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		• Оқшау пакеттерді тарату үшін веб-сервер порттарын көрсету: **Жазу** • MDM профильдерін тарату үшін веб-сервер порттарын көрсету: **Жазу** • Kaspersky Security Center Web Console арқылы қосылу үшін басқару серверінің SSL порттарын көрсету: **Жазу** • Мобильдік байланыс үшін басқару серверінің порттарын көрсету: **Жазу** • Басқару сервері дерекқорында сақталған оқиғалардың максималды санын көрсету: **Жазу** • Басқару сервері жібере алатын оқиғалардың максималды санын көрсету: **Жазу** • Басқару сервері оқиғаларды жібере алатын уақыт аралығын көрсету: **Жазу**			
Жалпы функционал: Kaspersky қолданбасын енгізу	• **Kaspersky патчтарын басқару** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	Патч орнатуды мақұлдау немесе қабылдамау: **Kaspersky патчтарын басқару**	Жоқ	• "Виртуалды Басқару серверінің лицензиялық кілтін пайдалануы туралы есеп" • "Kaspersky бағдарламалық жасақтамасының нұсқалары туралы есеп" • "Үйлесімсіз қосымшалар туралы есеп" • "Kaspersky бағдарламалық жасақтама модулі жаңартуларының нұсқалары туралы есеп" • "Қорғаныс орналастыру туралы есеп"	Орнату п Kaspersk
Жалпы функционал: Лицензиялық кілттерді басқару	• **Кілт файлын экспорттау** • **Жазу**	• Кілт файлын экспорттау: **Кілт файлын экспорттау** • Басқару серверінің лицензия кілтінің параметрлерін өзгерту: **Жазу**	Жоқ	Жоқ	Жоқ
Жалпы функционал: Есеп файлын мәжбүрлеп басқару	• **Оқу** • **Жазу**	• ACL-ге қарамастан есептерді жасау: **Жазу** • ACL-ге қарамастан есептерді орындау:	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		Оқу			

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
Жалпы функционал: Басқару серверлерінің иерархиясы	**Басқару серверлерінің иерархиясын конфигурациялау**	Қосалқы басқару серверлерін тіркеу, жаңарту немесе жою: **Басқару серверлерінің иерархиясын конфигурациялау**	Жоқ	Жоқ	Жоқ
Жалпы функционал: Пайдаланушы рұқсаттары	**Нысан ACL параметрлерін өзгерту**	• Кез келген нысанның қауіпсіздігі сипаттарын өзгерту: **Нысан ACL параметрлерін өзгерту** • Пайдаланушы рөлдерін басқару: **Нысан ACL параметрлерін өзгерту** • Ішкі пайдаланушыларды басқару: **Нысан ACL параметрлерін өзгерту** • Қауіпсіздік топтарын басқару: **Нысан ACL параметрлерін өзгерту** • Бүркеншік аттарды басқару: **Нысан ACL параметрлерін өзгерту**	Жоқ	Жоқ	Жоқ
Жалпы функционал: Виртуалды Басқару серверлері	• **Виртуалды Басқару серверлерін басқару** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Виртуалды басқару серверлерінің тізімін алу: **Оқу** • Виртуалды басқару сервері туралы ақпаратты алу: **Оқу** • Виртуалды басқару серверін жасау, жаңарту немесе жою: **Виртуалды Басқару серверлерін басқару** • Виртуалды басқару серверін басқа топқа жылжыту: **Виртуалды Басқару серверлерін басқару** • Виртуалды басқару сервері рұқсаттарын орнату: **Виртуалды Басқару серверлерін басқару**	Жоқ	Үшінші тарап бағдарламалық жасақтамасы жаңартуларын орнату нәтижелерін хабарлау.	Жоқ
Жалпы функционал: Шифрлау кілтін басқару	• **Оқу** • **Жазу**	• Шифрлау кілттерін экспорттау: **Оқу** • Шифрлау кілттерін импорттау: **Жазу**	Жоқ	Жоқ	Жоқ
Мобильді құрылғыларды басқару: Жалпы	• **Жаңа құрылғыларды қосу** • **Ұялы құрылғыларға тек**	• Key Management Service қалпына келтіру деректерін алу: **Оқу** • Пайдаланушы	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
	ақпараттық пәрмендерді жіберу • **Ұялы құрылғыларға пәрмендер жіберу** • **Сертификаттарды басқару** • **Оқу** • **Жазу**	сертификаттарын жою: **Сертификаттарды басқару** • Пайдаланушы сертификатының жалпы бөлігін алу: **Оқу** • Ашық кілт инфрақұрылымы қосылғанын тексеру: **Оқу** • Ашық кілт инфрақұрылымы есептік жазбасын тексеру: **Оқу** • Ашық кілт инфрақұрылымының үлгілерін алу: **Оқу** • Кеңейтілген кілтті пайдалану сертификаты арқылы ашық кілт инфрақұрылымының үлгілерін алу: **Оқу** • Ашық кілт инфрақұрылымы сертификатының күші жойылғанын тексеру: **Оқу** • Пайдаланушы сертификатын шығару параметрлерін жаңарту: **Сертификаттарды басқару** • Пайдаланушы сертификатын шығару параметрлерін алу: **Оқу** • Қолданба атауы мен нұсқасы бойынша пакеттерді алу: **Оқу** • Пайдаланушы сертификатын орнату немесе одан бас тарту: **Сертификаттарды басқару** • Пайдаланушы сертификатын жаңарту: **Сертификаттарды басқару** • Пайдаланушы сертификатының тэгін орнату: **Сертификаттарды басқару** • MDM орнату пакетін қайта жасауды іске қосу; MDM орнату пакетін жасаудан бас тарту: **Жаңа құрылғыларды қосу**			
Жүйені басқару: Қосылым мүмкіндігі	• **RDP сеанстарын бастау** • **Бұрыннан бар RDP сеанстарына қосылу**	• Жұмыс үстелін бөлісу сеансын жасау: **RDP сеанстарын бастау** • RDP сеансын жасау:	Жоқ	"Құрылғы пайдаланушылары туралы есеп"	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
	• **Туннельдеуді бастау** • **Құрылғылардағы файлдарды әкімшінің жұмыс станциясында сақтау** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	**Бұрыннан бар RDP сеанстарына қосылу** • Туннель жасау: **Туннельдеуді бастау** • Мазмұн желісінің тізімін сақтау: **Құрылғылардағы файлдарды әкімшінің жұмыс станциясында сақтау**			
Жүйені басқару: Жабдықты түгендеу	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Аппараттық жасақтаманы түгендеу нысанын алу немесе экспорттау: **Оқу** • Аппараттық жасақтаманы түгендеу нысанын қосу, орнату немесе жою: **Жазу**	Жоқ	• "Жабдық тізімдемесі туралы есеп" • "Конфигурацияны өзгерту туралы есеп" • "Жабдық туралы есеп"	Жоқ
Жүйені басқару: Желіге қатынасты басқару	• **Оқу** • **Жазу**	• CISCO параметрлерін көру: **Оқу** • CISCO параметрлерін өзгерту: **Жазу**	Жоқ	Жоқ	Жоқ
Жүйені басқару: Операциялық жүйені орналастыру	• **PXE серверлерін жаю** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• PXE серверлерін орналастыру: **PXE серверлерін жаю** • PXE серверлерінің тізімін көру: **Оқу** • PXE клиенттерінде орнату процесін бастау немесе тоқтату: **Орындау** • WinPE және операциялық жүйе кескіндері үшін драйверлерді басқару: **Жазу**	"Анықтамалық құрылғының ОЖ кескінінің орнату пакетін жасау"	Жоқ	Орнату п "Операци жүйе кес
Жүйені басқару: Осалдықтар мен патчтарды басқару	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Үшінші тарап патч сипаттарын көру: **Оқу** • Үшінші тарап патч сипаттарын өзгерту: **Жазу**	• "Windows Update жаңартуларын синхрондауды орындау" • "Windows Update жаңартуларын орнату" • "Осалдықтарды түзету" • "Қажетті жаңартуларды орнату және осалдықтарды түзету"	"Бағдарламалық жасақтаманың жаңартулары туралы есеп"	Жоқ
Жүйені басқару: Қашықтан орнату	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Үшінші тараптың осалдықтар мен патчтарды басқару негізіндегі орнату пакетінің сипаттарын көру: **Оқу** • Үшінші тараптың салдықтар мен патчтарды басқару негізіндегі орнату	Жоқ	Жоқ	Орнату п • "Пайд бағда • "Орна

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Ба
		пакетінің сипаттарын өзгертіңіз: **Жазу**			
Жүйені басқару: Бағдарламалық жасақтамаларды түгендеу	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	Жоқ	Жоқ	• "Орнатылған бағдарламалар туралы есеп" • "Өтінімдер тізілімі туралы есеп журналы" • "Лицензияланған бағдарламалар топтарының күйі туралы есеп" • "Үшінші тарап бағдарламалық жасақтамасының лицензиялық кілттері туралы есеп"	Жоқ

Алдын ала анықталған пайдаланушы рөлдері

Kaspersky Security Center пайдаланушыларына тағайындалған пайдаланушы рөлдері оларға бағдарламаның функцияларына қатынасу құқықтарының жиынтығын береді.

Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Конфигурацияланған құқықтар жинағы бар алдын ала анықталған пайдаланушы рөлдерін пайдалануға немесе жаңа рөлдер жасауға болады. Жаңа рөл жасаған кезде, рөл ауқымын өзіңіз орнатуыңыз және пайдалану құқықтарын Kaspersky Security Center мүмкіндіктеріне тағайындауыңыз керек. Kaspersky Security Center-де қолжетімді пайдаланушылардың кейбір алдын ала анықталған рөлдері **Аудитор**, **Қауіпсіздік қызметінің офицері**, **Супервайзер** сияқты белгілі бір лауазымдармен байланысты болуы мүмкін (бұл рөлдер Kaspersky Security Center бағдарламасында 11-нұсқадан бастап бар). Бұл рөлдерге қатынасу құқықтары тиісті лауазымдардың стандартты тапсырмалары мен міндеттеріне сәйкес алдын ала конфигурацияланады. Төмендегі кестеде рөлдердің белгілі бір лауазымдармен қалай байланысты болуы мүмкін екендігі көрсетілген.

Белгілі бір лауазымдарға арналған рөлдердің мысалдары

Рөл	Пікір
Аудитор	Басқару серверіне жергілікті әкімші құқықтары (Linux жүйесіне арналған түбір) бар желілік агент арқылы қосылған құрылғылар жинағында барлық көру операциясына және жасалған тапсырмаларды орындауға рұқсат береді. Бұл қызметтік міндеттерді орындау үшін осы рөлді пайдаланушылардың шектеулі жинағына мұқият тағайындауға кеңес береміз.
Супервайзер	Барлық операцияларды қарауға рұқсат етіледі, басқа операцияларға рұқсат етілмейді. Сіз бұл рөлді қауіпсіздік қызметінің офицеріне және ұйымыңыздағы IT қауіпсіздігіне жауап беретін басқа менеджерлерге тағайындай аласыз.
Қауіпсіздік қызметінің офицері	Барлық қарау операцияларына рұқсат етіледі, есептерді басқаруға рұқсат етіледі; **Жүйені басқару**: **Қосылым мүмкіндігі** аймағындағы шектулі құқықтар ұсынған. Сіз бұл рөлді ұйымыңыздағы IT қауіпсіздігіне жауапты қызметкерге тағайындай аласыз.

Төмендегі кестеде пайдаланушының әрбір алдын ала анықталған рөліне арналған құқықтар келтірілген.

Рөл	Сипаттамасы
Басқару серверінің әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Оқиғаларды өңдеу** • **Басқару серверлерінің иерархиясы** • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Қосылымдар** • **Жабдықты түгендеу** • **Бағдарламалық жасақтамаларды түгендеу** **Жалпы мүмкіндіктер: Шифрлау кілтін басқару** функционалды аймағында **Оқу** және **Жазу** құқықтарын береді.
Басқару серверінің операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Қосылымдар** • **Жабдықты түгендеу** • **Бағдарламалық жасақтамаларды түгендеу**
Аудитор	**Жалпы функционал** функционалдық аймағында барлық операцияларға рұқсат береді: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Жойылған нысандар** • **Есептерді басқару** Сіз бұл рөлді ұйымыңыздың аудитін жүргізетін қызметкерге тағайындай аласыз.
Бағдарламаларды орнату әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Kaspersky бағдарламалық жасақтамасын орналастыру** • **Лицензиялық кілттерді басқару** • **Жүйені басқару**: • **Операциялық жүйені орналастыру** • **Осалдықтар мен патчтарды басқару** • **Қашықтан орнату** • **Бағдарламалық жасақтамаларды түгендеу** **Жалпы функционал: Базалық функционалдылық** аймағында **Оқу** және **Орындау** құқықтарын ұсынады.

Рөл	Сипаттамасы
Бағдарламаларды орнату операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Kaspersky бағдарламалық жасақтамасын орналастыру** (сондай-ақ осы аймақта **Kaspersky патчтарын басқару** құқығын береді) • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Операциялық жүйені орналастыру** • **Осалдықтар мен патчтарды басқару** • **Қашықтан орнату** • **Бағдарламалық жасақтамаларды түгендеу**
Kaspersky Endpoint Security әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы **Жалпы мүмкіндіктер: Шифрлау кілтін басқару** функционалды аймағында **Оқу** және **Жазу** құқықтарын береді.
Kaspersky Endpoint Security операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функционал: Базалық функционал** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы
Бас әкімші	Келесі аймақтарды *қоспағанда*, функционалдық аймақтардағы барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Есептерді басқару** **Жалпы мүмкіндіктер: Шифрлау кілтін басқару** функционалды аймағында **Оқу** және **Жазу** құқықтарын береді.
Бас оператор	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Жойылған нысандар** • **Басқару серверіне қатысты әрекеттер** • **Kaspersky қолданбасын енгізу** • **Виртуалды Басқару серверлері** • **Ұялы құрылғыларды басқару: Жалпы** • Барлық функцияларды қосқанда, **Жүйені басқару** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы
Ұялы құрылғыларды басқару әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал** • **Ұялы құрылғыларды басқару: Жалпы**
Ұялы құрылғыларды басқару операторы	**Жалпы функционал**: **Базалық функционалдылық** аймағында **Оқу** және **Орындау** құқықтарын ұсынады. Келесі функционалдық аймақта **Оқу** және **Ұялы құрылғыларға тек ақпараттық пәрмендерді жіберу** құқықтарын ұсынады: **Ұялы құрылғыларды басқару**: **Жалпы**.

Рөл	Сипаттамасы
Қауіпсіздік қызметінің офицері	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Есептерді басқару** **Жүйені басқару: Қосылымдар** аймағында **Оқу**, **Жазу**, **Орындау**, **Құрылғылардағы файлдарды әкімшінің жұмыс орнында сақтау** және **Құрылғылардың таңдауларында әрекеттерді орындау** құқықтарын ұсынады. Сіз бұл рөлді ұйымыңыздағы IT қауіпсіздігіне жауапты қызметкерге тағайындай аласыз.
Self Service Portal пайдаланушысы	**Ұялы құрылғыларды басқару: Self Service Portal** аймағында барлық операцияларға рұқсат береді. Бұл функцияға Kaspersky Security Center 11 және одан жоғары нұсқаларында қолдау көрсетілмейді.
Супервайзер	**Жалпы функционал**: **ACL тізіміне қарамастан, нысандарға қатынасу** және **Жалпы функционал**: **Есептерді басқару** функционалдық аймағының аймағында **Оқу** құқықтарын ұсынады. Сіз бұл рөлді қауіпсіздік қызметінің офицеріне және ұйымыңыздағы IT қауіпсіздігіне жауап беретін басқа менеджерлерге тағайындай аласыз.
Осалдықтар мен патчтарды басқару әкімшісі	**Жалпы функционал**: **Базалық функционалдылық** және **Жүйені басқару** (барлық функцияларды қоса алғанда) аймағындағы барлық операцияларға рұқсат береді.
Осалдықтар мен патчтарды басқару операторы	**Жалпы функционал**: **Базалық функционалдылық** және **Жүйені басқару** (барлық функцияларды қоса алғанда) аймағында **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады.

Пайдаланушы рөлін қосу

Пайдаланушы рөлін қосу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Пайдаланушы рөлдері** бөліміне өтіп, **Қосылуда** түймесін басыңыз.

   > Қауіпсіздік параметрлері бар тарауларды көрсету параметрі қосулы болса, **Пайдаланушы рөлдері** бөлімі қолжетімді болады.

4. **Жаңа рөл** терезесінде рөл параметрлерін конфигурациялаңыз:

   - **Бөлімдер** панелінде **Жалпы** бөлімін таңдап, рөл атауын көрсетіңіз.

     Рөлдің атауы 100 таңбадан артық бола алмайды.

   - **Құқықтар** бөлімінде, бағдарлама функцияларына қарама-қарсы **Рұқсат** және **Тыйым салу** жалаушаларын қойып, құқықтар жиынтығын конфигурациялаңыз.

   Негізгі басқару серверінде жұмыс істесеңіз, **Рөлдер тізімін қосымша басқару серверлеріне жіберу** опциясын қосуға болады.

5. **ОК** түймесін басыңыз.

   Рөл қосылды.

Басқару сервері үшін жасалған пайдаланушы рөлдері **Пайдаланушы рөлдері** бөліміндегі Сервер сипаттары терезесінде көрсетіледі. Пайдаланушы рөлдерін өзгертуге және жоюға, сондай-ақ қауіпсіздік топтарына немесе жеке пайдаланушыларға рөлдерді тағайындауға болады.

Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау

Пайдаланушыға немесе пайдаланушылар тобына рөл тағайындау үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде **Қауіпсіздік** бөлімін таңдаңыз.

   Қауіпсіздік бөлімі, интерфейс параметрлері терезесінде **Қауіпсіздік параметрлері бар тарауларды көрсету** жалаушасы қойылса қолжетімді болады.

4. **Топтардың немесе пайдаланушылардың аттары** өрісінде рөл тағайындалатын пайдаланушыны немесе пайдаланушылар тобын таңдаңыз.

   Егер пайдаланушы немесе топ өрісте болмаса, оларды **Қосу** түймесі арқылы қосыңыз.

   Пайдаланушыны **Қосу** түймесі арқылы қосқан кезде пайдаланушы түпнұсқалық растамасы түрін таңдауға болады (Microsoft Windows немесе Kaspersky Security Center). Kaspersky Security Center түпнұсқалық растамасы виртуалды Басқару серверлерімен жұмыс істеу үшін пайдаланылатын ішкі пайдаланушы есептік жазбаларын таңдау үшін пайдаланылады.

5. **Рөлдер** қойыншасына өтіп, **Қосу** түймесін басыңыз.

   Пайдаланушы рөлдері терезесі ашылады. Терезеде жасалған пайдаланушы рөлдері көрсетіледі.

6. **Пайдаланушы рөлдері** терезесінде қауіпсіздік тобы үшін рөл таңдаңыз.
7. **OK** түймесін басыңыз.

Нәтижесінде басқару серверімен жұмыс істеу құқықтарының жиынтығы бар рөл пайдаланушыға немесе қауіпсіздік тобына тағайындалады. Тағайындалған рөлдер Басқару сервері сипаттары терезесінің **Қауіпсіздік** бөліміндегі **Рөлдер** қойыншасында көрсетіледі.

Пайдаланушыларға немесе пайдаланушылар топтарына құқықтарды тағайындау

Kaspersky Endpoint Security for Windows сияқты басқару плагиндеріңіз бар Kaspersky Басқару сервері мен бағдарламаларының әртүрлі мүмкіндіктерін пайдалану үшін пайдаланушыларға немесе пайдаланушы топтарына құқықтарды тағайындауға болады.

Пайдаланушыға немесе пайдаланушылар тобына құқықтарды тағайындау үшін:

1. Консоль ағашында келесі әрекеттердің бірін орындаңыз:
   - **Басқару сервері** түйінін ашыңыз және қажетті Басқару сервері деп аталатын ішкі қалтаны таңдаңыз.
   - Басқару тобын таңдаңыз.
2. Басқару серверінің немесе басқару тобының контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

3. Ашылған Басқару сервері сипаттары терезесінде (немесе басқару тобы сипаттары терезесінде) **Бөлімдер** панелінде **Қауіпсіздік** бөлімін таңдаңыз.

   Қауіпсіздік бөлімі, интерфейс параметрлері терезесінде **Қауіпсіздік параметрлері бар тарауларды көрсету** жалаушасы қойылса қолжетімді болады.

4. **Қауіпсіздік** бөліміндегі **Топтардың немесе пайдаланушылардың аттары** тізімінен пайдаланушыны немесе пайдаланушылар тобын таңдаңыз.

5. Терезенің төменгі бөлігіндегі құқықтар тізімінде, **Құқықтар** қойыншасында пайдаланушыларға немесе топтарға арналған құқықтарды конфигурациялаңыз:

   a. Тізімдегі түйінді ашу үшін плюс (+) белгішесін нұқыңыз және құқықтарды тағайындаңыз.

   b. Қажетті құқықтардың жанына **Рұқсат** және **Тыйым салу** жалаушаларын қойыңыз.

      1-мысал: **ACL тізіміне қарамастан, нысандарға қатынасу** түйінін немесе **Жойылған нысандар** түйінін ашып, **Оқу** тармағын таңдаңыз.

      2-мысал: **Базалық функционалдылық** түйінін ашып, **Жазу** тармағын таңдаңыз.

6. Құқықтар жиынтығын конфигурациялағаннан кейін, **Қолдану** түймесін басыңыз.

Пайдаланушы немесе пайдаланушылар тобы үшін құқықтар жиынтығы конфигурацияланған.

Басқару серверінің (немесе басқару тобының) құқықтары келесі аймақтарға бөлінеді:

- Жалпы функциялар:
  - Басқару топтарын басқару
  - ACL тізіміне қарамастан, нысандарға қатынасу
  - Базалық функционалдылық
  - Жойылған нысандар
  - Оқиғаларды өңдеу
  - Басқару серверіне қатысты әрекеттер (тек Басқару сервері сипаттары терезесінде)
  - Kaspersky қолданбаларын орналастыру
  - Лицензиялық кілттерді басқару
  - Есептерді басқару
  - Серверлер иерархиясы
  - Пайдаланушылар құқықтары
  - Виртуалды Басқару серверлері

- Ұялы құрылғыларды басқару:
  - Жалпы
- Жүйені басқару:
  - Қосылымдар
  - Жабдықты түгендеу
  - Желіге қатынасуды басқару
  - Операциялық жүйені орналастыру
  - Осалдықтар мен патчтарды басқару
  - Қашықтан орнату
  - Бағдарламалық жасақтамаларды түгендеу

Құқық үшін не **Рұқсат**, не **Тыйым салу** таңдалмаса, ол *анықталмаған* болып саналады: құқық пайдаланушы үшін айқын түрде қабылданбайынша немесе рұқсат етілмейінше қабылданбайды.

Пайдаланушылардың құқықтары келесінің жиынтығы болып саналады:

- Пайдаланушының өзіндік құқықтары
- Пайдаланушыға тағайындалған барлық рөлдердің құқықтары
- Пайдаланушы кіретін барлық қауіпсіздік топтарының құқықтары
- Пайдаланушы кіретін топтарға тағайындалған барлық рөлдердің құқықтары

Ең болмаса бір құқықтар жиынтығында тыйым салынған құқық болса (құқық үшін **Тыйым салу** жалаушасы қойылған), онда бұл құқық басқа құқықтар жиынтығында рұқсат етілген немесе анықталмаған болса да, пайдаланушы үшін тыйым салынған болып саналады.

Қосалқы Басқару серверлеріне пайдаланушы рөлдерін тарату

Әдепкі бойынша, негізгі және қосалқы Басқару серверлерінің пайдаланушы рөлдерінің тізімдері тәуелсіз болып саналады. Негізгі Басқару серверінде жасалған пайдаланушы рөлдерін барлық Басқару серверіне автоматты түрде тарату үшін бағдарламаларды орнатуға болады. Пайдаланушы рөлдері қосалқы Басқару серверінен өзінің қосалқы Басқару серверлеріне де таралуы мүмкін.

Пайдаланушы рөлдерін негізгі Басқару серверінен қосалқы Басқару серверлеріне тарату үшін:

1. Бағдарламаның басты терезесін ашыңыз.
2. Келесі әрекеттердің бірін орындаңыз:
   - Консоль ағашында қажетті Басқару серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
   - Егер сізде белсенді Басқару сервері саясаты болса, **Саясаттар** қалтасының жұмыс аймағында осы саясаттың контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесінде немесе саясат сипаттары терезесінде **Бөлімдер** панелінде **Пайдаланушы рөлдері** бөліміне өтіңіз.

   [Қауіпсіздік параметрлері бар тарауларды көрсету](#) параметрі қосулы болса, **Пайдаланушы рөлдері** бөлімі қолжетімді болады.

4. **Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу** параметрін қосыңыз.

5. **OK** түймесін басыңыз.

Бағдарлама негізгі Басқару сервері пайдаланушыларының рөлдерін қосалқы Басқару серверлеріне көшіреді.

Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу параметрі қосулы және пайдаланушы рөлдері таратылған болса, мұндай рөлдер қосалқы Басқару серверінде өзгерту немесе жою үшін қолжетімді емес. Негізгі Басқару серверінде рөл жасағанда немесе қолданыстағы рөлді өзгерткенде, өзгерістер автоматты түрде қосалқы Басқару серверлеріне көшіріледі. Негізгі Басқару серверінде пайдаланушы рөлін жойған кезде, бұл рөл қосалқы Басқару серверінде қалады және оны өзгертуге немесе жоюға болады.

Басты серверден қосалқы Басқару серверіне таралатын рөлдер құлып белгішесі (🔒) арқылы көрсетіледі. Сіз бұл рөлдерді қосалқы Басқару серверінде өзгерте алмайсыз.

Егер рөл негізгі Басқару серверінде жасалса және қосалқы Басқару серверінде бірдей атауы бар рөл болса, жаңа рөл қосалқы Басқару серверіне көшіріледі және оның атына жақшаға нөмір қосылады, мысалы, ~~1, ~~2 (нөмірі кездейсоқ болуы мүмкін).

Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу параметрін өшірсеңіз, барлық пайдаланушы рөлдері қосалқы Басқару серверлерінде қала береді, бірақ негізгі Басқару серверіндегі рөлдерден тәуелсіз болады. Қосалқы Басқару серверлеріндегі рөлдер тәуелсіз болған кезде, оларды өзгертуге немесе жоюға болады.

Пайдаланушыны құрылғының иесі етіп тағайындау

Құрылғыны пайдаланушыға "бекіту" үшін осы пайдаланушыны құрылғы иесі етіп тағайындауға болады. Құрылғымен қандай да бір әрекеттерді орындау қажет болса (мысалы, аппараттық жасақтаманы жаңарту), әкімші құрылғы иесіне хабарлап, онымен әрекеттерді үйлестіре алады.

Пайдаланушыны ұялы құрылғының иесі етіп тағайындау үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.

2. Қалтаның жұмыс аймағында, **Құрылғылар** қойыншасында иесін тағайындау үшін құрылғыны таңдаңыз.

3. Құрылғының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.

4. Құрылғы сипаттары терезесінде **Жүйе ақпараты** → **Сеанстар** тармағын таңдаңыз.

5. **Құрылғының иесі** өрісінің жанындағы **Белгілеу** түймесін басыңыз.

6. **Пайдаланушыны таңдау** терезесінде құрылғының иесі етіп тағайындау қажет пайдаланушыны таңдап, **OK** түймесін басыңыз.

7. **OK** түймесін басыңыз.

Нәтижесінде, құрылғы иесі тағайындалады. Әдепкі бойынша, **Құрылғының иесі** өрісі Active Directory ішіндегі мәнмен толтырылған және әрбір Active Directory сауалнамасы кезінде жаңартылады. Сіз құрылғы иелері тізімін **Құрылғылар иесі туралы есеп** есебінде қарап шыға аласыз. Есепті есептер жасау шебері арқылы жасай аласыз.

Пайдаланушыларға хабарлар жіберу

Пайдаланушыға электрондық пошта арқылы хабар жіберу үшін:

1. Консоль ағашының **Пайдаланушылардың есептік жазбалары** қалтасында пайдаланушыны таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Пайдаланушы контекстік мәзірінде **Электрондық пошта арқылы хабарлау** таңдаңыз.

3. **Пайдаланушыға хабар жіберу** терезесінде қажетті өрістерді толтырып, **OK** түймесін басыңыз.

Нәтижесінде, хабар пайдаланушының сипаттарында көрсетілген электрондық поштаға жіберіледі.

Пайдаланушыға SMS-хабар жіберу үшін:

1. Консоль ағашының **Пайдаланушылардың есептік жазбалары** қалтасында пайдаланушыны таңдаңыз.

2. Пайдаланушы контекстік мәзірінде **SMS хабарын жіберу** таңдаңыз.

3. **SMS мәтіні** терезесінде қажетті өрістерді толтырып, **OK** түймесін басыңыз.

Нәтижесінде, хабар, нөмірі пайдаланушының сипаттарында көрсетілген ұялы құрылғыға жіберіледі.

Пайдаланушының ұялы құрылғылар тізімін қарау

Пайдаланушының ұялы құрылғыларының тізімін көру үшін:

1. Консоль ағашының **Пайдаланушылардың есептік жазбалары** қалтасында пайдаланушыны таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Пайдаланушының есептік жазбасы сипаттары терезесінде **Ұялы құрылғылар** бөлімін таңдаңыз.

Ұялы құрылғылар бөлімінде пайдаланушының ұялы құрылғыларының тізімін және ұялы құрылғылар туралы ақпаратты көруге болады. **Файлға экспорттау** түймесі арқылы файлдағы ұялы құрылғылар тізімін сақтауға болады.

Пайдаланушыға сертификатты орнату

Пайдаланушыға сертификаттардың үш түрін орнатуға болады:

- пайдаланушының ұялы құрылғысын анықтау үшін қажет жалпы сертификат;
- пошта сертификаты, пайдаланушының ұялы құрылғысында корпоративтік поштаны конфигурациялау үшін қажет;
- VPN сертификаты, пайдаланушының ұялы құрылғысында виртуалды жеке желіні конфигурациялау үшін қажет.

Пайдаланушы сертификатын жазып беру және оны орнату үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын ашып, пайдаланушы есептік жазбасын таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Сертификатты орнату** тармағын таңдаңыз.

Сертификаттарды орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Сертификаттарды орнату шебері жұмысы нәтижесінде, сертификат жасалып, пайдаланушыға орнатылады. Пайдаланушының орнатылған сертификаттары тізімін қарап шығып, файлға экспорттауға болады.

Пайдаланушыға жазылған сертификаттар тізімін қарау

Пайдаланушыға жазылған барлық сертификаттардың тізімін қарау үшін:

1. Консоль ағашының **Пайдаланушылардың есептік жазбалары** қалтасында пайдаланушыны таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Пайдаланушының есептік жазбасы сипаттары терезесінде **Сертификаттар** бөлімін таңдаңыз.

Сертификаттар бөлімінде пайдаланушы сертификаттарының тізімін және сертификат туралы ақпаратты көруге болады. **Файлға экспортталуда** түймесі арқылы сертификаттар тізімін файлға сақтауға болады.

Виртуалды Басқару сервері әкімшісі туралы

Виртуалды Сервер басқаратын ұйым желісі әкімшісі осы терезеде көрсетілген есептік жазба атауымен желінің антивирустық қорғанысының күйі туралы мәліметтерді көру үшін Kaspersky Security Center Web Console серверін іске қосады.

Қажет болса, бірнеше виртуалды сервер әкімші есептік жазбаларын жасауға болады.

Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Виртуалды Басқару сервері әкімшісі Kaspersky Security Center ішкі пайдаланушысы болып табылады. Ішкі пайдаланушылар туралы мәліметтер операциялық жүйеге берілмейді. Ішкі пайдаланушылардың аутентификациясын Kaspersky Security Center жүзеге асырады.

Операциялық жүйелер мен бағдарламаларды қашықтан орнату

Kaspersky Security Center бағдарламасы операциялық жүйелердің кескіндерін орталықтандырылған түрде жасауға және оларды желі арқылы клиент құрылғыларына орналастыруға, сонымен қатар Kaspersky немесе басқа да бағдарламалық жасақтама өндірушілерінің бағдарламаларын қашықтан орнатуға мүмкіндік береді.

Операциялық жүйелердің кескіндерін жасау үшін Басқару серверлерінде Windows ADK және Windows ADK үшін Windows PE толықтыруларын орнатыңыз. Kaspersky Security Center талаптарына сай келетін Windows операциялық жүйесінің кез келген нұсқасының кескінін жасай аласыз.

Kaspersky Security Center бағдарламасы Windows ADK және Windows PE жүйесінің 64 разрядтық нұсқаларына қолдау көрсетпейді.

Операциялық жүйенің кескіндерін қармау

Kaspersky Security Center құрылғылардың операциялық жүйелерінің кескіндерін қармай алады және бұл кескіндерді Басқару серверіне жеткізе алады. Мұндай операциялық жүйелердің кескіндері Басқару серверінде арнайы қалтада сақталады. Эталондық құрылғының операциялық жүйесінің кескінін алу және жасау орнату пакетін жасау тапсырмасы арқылы жүзеге асырылады.

Операциялық жүйенің кескінін қармау функционалдығы келесі ерекшеліктерге ие:

- Операциялық жүйенің кескінін Басқару сервері орнатылған құрылғыдан алып тастауға болмайды.
- Операциялық жүйенің кескінін түсіру кезінде sysprep.exe утилитасы эталондық құрылғының параметрлерін нөлге айналдырады. Операциялық жүйенің кескінін алу тапсырмасын жасау шеберінде эталондық құрылғының параметрлерін қалпына келтіру қажет болған жағдайда **Құрылғы күйінің сақтық көшірмесін жасау** жалаушасын қою керек.
- Кескінді алу процесінде эталондық құрылғы қайта іске қосылады.

Жаңа құрылғыларда операциялық жүйе кескіндерін орналастыру

Алынған кескіндерді, операциялық жүйе әлі орнатылмаған желідегі жаңа құрылғыларға орналастыру үшін пайдалануға болады. Осы мақсатта Preboot eXecution Environment (PXE) технологиясы қолданылады. Сіз құрылғыны PXE сервері ретінде пайдаланылатын желіге тағайындайсыз. Бұл құрылғы келесі талаптарға сай болуы керек:

- құрылғыға Желілік агент орнатылуы керек;
- құрылғыда DHCP сервері жұмыс істемеуі керек, өйткені PXE сервері DHCP сияқты бірдей порттарды пайдаланады;
- құрылғы кіретін желі сегментінде басқа PXE серверлері болмауы керек.

Операциялық жүйені орналастыру үшін келесі шарттар орындалуы керек:

- құрылғыда желілік карта орнатылуы керек;
- құрылғы желіге қосылуы керек;
- құрылғыны BIOS-қа жүктеген кезде желі арқылы жүктеу параметрін таңдау керек.

Операциялық жүйені орналастыру келесі ретпен жүзеге асырылады:

1. Клиент құрылғысы жүктелген кезде клиент құрылғысы PXE серверімен қосылым орнатады.
2. Клиент құрылғысы Windows Preinstallation Environment (WinPE) ортасында жүктеледі.

   Құрылғыны WinPE ортасына қосу мақсатында WinPE ортасы үшін драйвер құрамын конфигурациялау қажет болуы мүмкін.

3. Клиент құрылғысы Басқару серверінде тіркеледі.
4. Әкімші клиент құрылғысына операциялық жүйенің кескіні бар орнату пакетін тағайындайды.

   Әкімші операциялық жүйенің кескіні бар орнату пакетіне қажетті драйверлерді қоса алады. Сондай-ақ, әкімші орнату кезінде қолданылуы керек операциялық жүйенің параметрлері (жауаптар файлы) бар конфигурация файлын көрсете алады.

5. Операциялық жүйені клиент құрылғысына орналастыру жүзеге асырылады.

Әкімші әлі қосылмаған клиент құрылғыларының MAC мекенжайларын қолмен көрсете алады және оларға операциялық жүйенің кескіні бар орнату пакетін тағайындай алады. Көрсетілген клиент құрылғылары PXE серверіне қосылған кезде, бұл құрылғыларда операциялық жүйе автоматты түрде орнатылады.

Қазірдің өзінде орнатылған операциялық жүйесі бар құрылғыларда операциялық жүйелердің кескіндерін орналастыру

Операциялық жүйенің кескіндерін жұмысқа жарамды операциялық жүйесі орнатылған клиент құрылғыларына орналастыру арнайы құрылғылар үшін қашықтан орнату тапсырмасы арқылы жүзеге асырылады.

Операциялық жүйені таза орнату орындалып жатқанын ескеріңіз. Барлық деректер жойылады.

Kaspersky және басқа да үшін бағдарламалық жасақтама өндірушілерінің бағдарламаларын орнату

Әкімші кез келген бағдарламаның, соның ішінде пайдаланушы көрсеткен бағдарламалардың орнату пакеттерін жасай алады және сол бағдарламаларды қашықтан орнату тапсырмасы арқылы клиент құрылғыларына орната алады.

Операциялық жүйенің кескіндерін жасау

Операциялық жүйелердің кескіндерін жасау, эталондық құрылғының операциялық жүйесінің кескінін алу тапсырмасын қолдана отырып жүзеге асырылады.

Операциялық жүйенің кескінін алу тапсырмасын жасау үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
2. **Орнату пакетін жасау** түймесі арқылы орнату пакетін жасау шеберін іске қосыңыз.
3. Шебердің **Орнату пакетінің түрін таңдау** терезесінде **Операциялық жүйе кескіні бар орнату пакетін жасау** түймесін басыңыз.
4. Содан кейін, шебердің нұсқауларын орындаңыз.

   Шебердің жұмысы нәтижесінде Басқару серверінің **Анықтамалық құрылғының ОЖ кескінінің орнату пакетін жасау** тапсырмасы жасалады. Тапсырманы **Тапсырмалар** қалтасында қарауға болады.

Анықтамалық құрылғының ОЖ кескінінің орнату пакетін жасау тапсырмасының орындалуы нәтижесінде, PXE серверін немесе қашықтан орнату тапсырмасын пайдаланып клиент құрылғыларында операциялық жүйені орналастыру үшін пайдалануға болатын орнату пакеті жасалады. Орнату пакетін **Орнату пакеттері** қалтасында қарап шығуға болады.

Операциялық жүйенің кескіндерін орнату

Kaspersky Security Center ұйым желісі құрылғыларына Windows операциялық жүйелерінің үстелдік және серверлік нұсқаларының wim-үлгілерін орналастыруға мүмкіндік береді.

Kaspersky Security Center құралдарымен орналастыруға жарамды операциялық жүйенің үлгісі келесі тәсілдермен алынуы мүмкін:

- Windows дистрибутивінің мазмұнына кіретін install.wim файлынан импорттау;
- эталондық құрылғыдан үлгіні қармау.

Операциялық жүйенің үлгісін орналастырудың екі сценарийіне қолдау көрсетіледі:

- "таза" құрылғыға, яғни операциялық жүйесі орнатылмаған құрылғыға орналастыру;
- Windows операциялық жүйесі басқарып жұмыс істейтін құрылғыға орналастыру.

Операциялық жүйе кескіндерін түсіру және орналастыру үшін Windows Preinstallation Environment (Windows PE) пайдаланыңыз. WinPE-де барлық құрылғылардың дұрыс жұмысына қажетті барлық драйверлерді қосу керек. Әдетте, желілік адаптер мен сақтау құрылғысының контроллері драйверлерін қосу керек.

Үлгілерді орналастыру және қармау сценарийлерін іске асыру үшін келесі талаптар орындалуы тиіс:

- Басқару серверінде Windows Automated Installation Kit (WAIK) 2.0 не одан жоғары нұсқасы немесе Windows ADK үшін Windows PE қондырмасы бар Windows ADK орнатылған болуы керек. Егер Windows XP-де үлгілерді орнату немесе қармау бойынша жұмыстар болжамданса, WAIK орнату керек.
- Құрылғы орналасқан желіде DHCP-сервер болуы керек.
- Басқару серверінің ортақ қатынас бар қалтасы құрылғы орналасқан желіден оқу үшін қолжетімді болуы тиіс. Егер ортақ қатынасы бар қалта Басқару серверінде орналасса, онда KlPxeUser есептік жазбасы үшін қатынас керек (бұл есептік жазба автоматты түрде Басқару сервері инсталляторының жұмысы кезеңінде жасалады). Егер қалта Басқару серверінде орналасса, онда қатынас барлығы үшін керек.

Орнату үшін операциялық жүйенің үлгісін таңдаған кезде әкімші құрылғы процессорының құрылымына айқын түрде көрсетуі тиіс: x86 немесе x86-64.

KSN прокси-сервері мекенжайын конфигурациялау

Әдепкі бойынша басқару серверінің қосылым атауы немесе IP мекенжайы KSN прокси серверінің мекенжайына сәйкес келеді. Басқару сервері үшін қосылым атауын өзгерткен кезде, құрылғылар мен KSN арасындағы байланыстың жоғалуына жол бермеу үшін дұрыс KSN прокси сервері мекенжайын көрсету керек.

KSN прокси-сервері мекенжайларын конфигурациялау үшін:

1. Консоль ағашында **Кеңейтілген** → **Қашықтан орнату** → **Орнату пакеттері** бөліміне өтіңіз.
2. **Орнату пакеттері** қалтасының контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
3. Ашылған терезеде, **Жалпы** қойыншасында KSN прокси-серверінің жаңа мекенжайын көрсетіңіз.
4. **Қолдану** түймесін басыңыз.

Осы сәттен бастап, көрсетілген мекенжай KSN прокси-серверінің мекенжайы ретінде қолданылады. Желілік трафикті оңтайландыру үшін **KSN прокси серверін** пайдалану параметрін қосу ұсынылады.

Windows жүйесін алдын ала орнату ортасының драйверлерін (WinPE) қосу

Windows жүйесін алдын ала орнату ортасының драйверлерін (WinPE) қосу үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Құрылғы кескіндерін орналастыру** салынған қалтасын таңдаңыз.
2. **Құрылғы кескіндерін орналастыру** қалтасының жұмыс аймағында **Қосымша әрекеттер** түймесін басып, ашылмалы тізімнен **Windows (WinPE) алдын ала орнату ортасы үшін драйверлер құрамын реттеу** тармағын таңдаңыз.

   Windows жүйесін алдын ала орнату ортасының драйверлері терезесі ашылады.
3. **Windows жүйесін алдын ала орнату ортасының драйверлері** терезесінде **Қосылуда** түймесін басыңыз.

   Драйверді таңдау терезесі ашылады.

4. **Драйверді таңдау** терезесінде тізімдегі драйверді таңдаңыз.

   Егер қажетті драйвер тізімде болмаса, **Қосылуда** түймесін басыңыз және ашылған **Драйверді қосу** терезесінде драйвер атауын және драйвердің тарату қалтасын көрсетіңіз.

   Қалтаны **Шолу** түймесі арқылы таңдай аласыз.

   Драйверді қосу терезесінде **OK** түймесін басыңыз.

5. **Драйверді таңдау** терезесінде **OK** түймесін басыңыз.

   Драйвер Басқару серверінің қоймасына қосылады. Қоймаға қосылған драйвер **Драйверді таңдау** терезесінде көрсетіледі.

6. **Windows жүйесін алдын ала орнату ортасының драйверлері** терезесінде **OK** түймесін басыңыз.

Драйвер Windows алдын ала орнату ортасына (WinPE) қосылады.

Драйверлерді операциялық жүйенің кескінімен орнату пакетіне қосу

Драйверлерді операциялық жүйенің кескіні бар орнату пакетіне қосу үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
2. Операциялық жүйенің орнату пакетінің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Орнату пакеті сипаттары терезесі ашылады.
3. Орнату пакеті сипаттары терезесінде **Қосымша драйверлер** бөлімін таңдаңыз.
4. **Қосымша драйверлер** бөлімінде орналасқан **Қосылуда** түймесін басыңыз.

   Драйверді таңдау терезесі ашылады.
5. **Драйверді таңдау** терезесінде операциялық жүйенің кескіні бар орнату пакетіне қосқыңыз келетін драйверлерді таңдаңыз.

   Жаңа драйверлерді, **Драйверді таңдау** терезесінде **Қосылуда** түймесін басу кезінде Басқару серверінің қоймасына қосуға болады.
6. **OK** түймесін басыңыз.

Қосылған драйверлер **Қосымша драйверлер** терезесінде, операциялық жүйенің кескіні бар орнату пакетінің сипаттары терезесінде көрсетіледі.

sysprep.exe утилитасы параметрлерін конфигурациялау

sysrep.exe утилитасы құрылғыны одан операциялық жүйенің кескінін жасауға дайындау үшін қолданылады.

sysprep.exe утилитасының параметрлерін конфигурациялау үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
2. Операциялық жүйенің орнату пакетінің контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Орнату пакеті сипаттары терезесі ашылады.
3. Орнату пакеті сипаттары терезесінде **sysprep.exe параметрлері** бөлімін таңдаңыз.

4. **sysprep.exe параметрлері** бөлімінде клиент құрылғысында операциялық жүйені орналастыру кезінде қолданылатын конфигурациялық файлды көрсетіңіз:

   - **Әдепкі конфигурациялық файлды пайдалану**. Операциялық жүйенің кескінін алу кезінде әдепкі бойынша жасалған жауап файлын қолдану үшін осы нұсқаны таңдаңыз.
   - **Негізгі параметрлердің пайдаланушылық мәндерін белгілеу**. Пайдаланушы интерфейсін пайдаланып параметрлер мәндерін белгілеу үшін осы нұсқаны таңдаңыз.
   - **Конфигурациялық файлды белгілеу**. Өзіндік жауап файлын пайдалану үшін осы нұсқаны таңдаңыз.

5. Енгізілген өзгерістер күшіне енуі үшін **Қолдану** түймесін басыңыз.

Операциялық жүйелерді желідегі жаңа құрылғыларға орналастыру

Операциялық жүйені операциялық жүйе әлі орнатылмаған жаңа құрылғыларға орналастыру үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Құрылғы кескіндерін орналастыру** салынған қалтасын таңдаңыз.

   Осалдықтар мен патчтарды басқаруды көрсету терезесінде **Интерфейсті конфигурациялау** опциясы қосылғанын тексеріңіз. Әйтпесе, **Қашықтан орнату** қалтасы көрсетілмейді.

2. **Қосымша әрекеттер** түймесін басыңыз да, ашылатын тізімнен **Желідегі PXE серверлер тізімін басқару** мәнін таңдаңыз.

   Сипаттар: PXE серверлері бөлімінде **Құрылғы кескіндерін орналастыру** терезесі ашылады.

3. **PXE серверлері** бөлімінде **Қосылуда** түймесін басыңыз және ашылған **PXE серверлері** терезесінде PXE сервері ретінде қолданылатын құрылғыны таңдаңыз.

   Қосылған құрылғы PXE серверлері бөлімінде көрсетіледі. Жасалған WinPE файлдары Басқару серверінен құрылғыға беріледі. Файлдарды беру процесі әдетте 10 минутты алады. Файлды беру аяқталғаннан кейін, көрсетілетін **Күйі** мәні **Жұмысқа кірісу** мәнінен **Дайын** мәніне өзгертіледі.

4. **PXE серверлері** бөлімінде PXE серверін таңдаңыз және **Сипаттар** түймесін басыңыз.

5. Таңдалған PXE серверінің сипаттар терезесінде **PXE серверіне қосылу параметрлері** бөлімінде Басқару серверін PXE серверіне қосу параметрлерін конфигурациялаңыз.

6. Операциялық жүйені орналастырғыңыз келетін клиент құрылғысын жүктеңіз.

7. Клиент құрылғысының BIOS ортасында Network boot орнату нұсқасын таңдаңыз.

   Клиент құрылғысы PXE серверіне қосылады және **Құрылғы кескіндерін орналастыру** қалтасының жұмыс аймағында көрсетіледі.

8. **Әрекеттер** блогында **Орнату пакетін белгілеу** сілтемесі арқылы таңдалған құрылғыға операциялық жүйені орнату үшін пайдаланылатын орнату пакетін таңдаңыз.

   Қолжетімді дискілерді тексеру үшін таңдалған құрылғыдағы DiskPart құралын пайдаланыңыз. Windows PE пәрмен жолында DiskPart құралын ашу үшін `diskpart` деп енгізіңіз. Дискілер тізімін көру үшін `list disk` енгізіңіз.

   Құрылғыны қосып, оған орнату пакетін тағайындағаннан кейін, операциялық жүйені осы құрылғыға орналастыру автоматты түрде басталады.

9. Операциялық жүйені клиент құрылғысында орналастыруды болдырмау үшін **Әрекеттер** блогында **Операциялық жүйе кескіндерін орнатудан бас тарту** сілтемесін пайдаланыңыз.

MAC мекенжайына құрылғыларды қосу үшін келесі әрекеттердің бірін орындаңыз:

- **Жаңа құрылғы** терезесін ашу үшін **Құрылғы кескіндерін орналастыру** қалтасындағы **Құрылғының MAC мекенжайын қосу** түймесін басып, қосқыңыз келген құрылғының MAC мекенжайын көрсетіңіз.
- Операциялық жүйені орналастырғыңыз келетін барлық құрылғының MAC мекенжайларының тізімін қамтитын файлды таңдау үшін **Құрылғы кескіндерін орналастыру** қалтасындағы **Файлдан құрылғылардың MAC мекенжайларын импорттау** түймесін басыңыз.

Клиент құрылғыларында операциялық жүйелерді орналастыру

Операциялық жүйені қазірдің өзінде орнатылған операциялық жүйесі бар клиент құрылғыларына орналастыру үшін:

1. Қорғанысты орналастыру шеберін іске қосу үшін консоль ағашында **Қашықтан орнату** қалтасын ашып, **Орнату пакетін басқарылатын құрылғыларда (жұмыс станциялары) орналастыру** сілтемесінен өтіңіз.
2. Шебердің **Орнату пакетін таңдау** терезесінде операциялық жүйенің кескіні бар орнату пакетін көрсетіңіз.
3. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысының нәтижесінде клиент құрылғыларында операциялық жүйені қашықтан орнату тапсырмасы жасалады. Тапсырманы **Тапсырмалар** қалтасында іске қосуға немесе тоқтатуға болады.

Бағдарламалардың орнату пакеттерін жасау

Бағдарламаның орнату пакетін жасау үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.
2. **Орнату пакетін жасау** түймесі арқылы орнату пакетін жасау шеберін іске қосыңыз.
3. Шебердің **Орнату пакетінің түрін таңдау** терезесінде келесі түймелердің бірін басыңыз:
   - **Kaspersky бағдарламасы үшін орнату пакетін жасаңыз**. Kaspersky бағдарламасы үшін орнату пакетін жасағыңыз келсе, осы нұсқаны таңдаңыз.
   - **Көрсетілген орындалатын файл үшін орнату пакетін жасаңыз**. Орындалатын файлды пайдаланып бағдарлама үшін орнату пакетін жасағыңыз келсе, осы нұсқаны таңдаңыз. Әдетте, орындалатын файл бағдарламаның орнату файлы болып табылады.
     - **Бүкіл қалтаны орнату пакетіне көшіру**

       Егер орындалатын файл бағдарламаны орнатуға қажетті қосымша файлдармен бірге жүрсе, осы параметрді таңдаңыз. Бұл параметрді қоспас бұрын, барлық қажетті файлдардың бір қалтада сақталғанына көз жеткізіңіз. Егер бұл параметр қосылса, бағдарлама орнату пакетіне қалтаның барлық ішіндегісін, соның ішінде көрсетілген орындалатын файлды қосады.

     - **Орнату параметрлерін көрсетіңіз**

       Қашықтан орнату сәтті өтуі үшін көптеген бағдарламалар орнатудың тыныш режимде жүргізілуін талап етеді. Бұл жағдайда автоматты түрде орнату параметрлерін көрсетуіңіз керек.

Орнату параметрлерін конфигурациялаңыз:

- **Орындалатын файлдың пәрмен жолы**

  Егер бағдарлама хабарларды көрсетпестен орнату үшін қосымша параметрлерді қажет етсе, оларды осы өрісте көрсетіңіз. Қосымша ақпарат алу үшін өндірушінің құжаттамасын қараңыз.

  Сіз басқа параметрлерді де көрсете аласыз.

- **Параметрлерді Kaspersky Security Center нұсқасы анықтай алатын бағдарламалар үшін ұсынылатын мәндерге түрлендіру**

  Егер аталған бағдарлама туралы ақпарат Kaspersky дерекқорында болса, бағдарлама ұсынылған параметрлермен орнатылады.

  Егер сіз **Орындалатын файлдың пәрмен жолы** өрісіне параметрлерді енгізсеңіз, олар ұсынылған параметрлерге өзгертіледі.

  Әдепкі бойынша, параметр қосулы.

  Kaspersky дерекқорын Kaspersky талдаушылары құрды және қолдайды. Дерекқорға қосылатын әрбір бағдарлама үшін Kaspersky талдаушылары орнатудың оңтайлы параметрлерін анықтайды. Параметрлер, клиент құрылғысына бағдарламаны қашықтан сәтті орнатуды қамтамасыз ететіндей етіп анықталады. Дерекқор Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын іске қосу кезінде автоматты түрде жаңартылады.

- **Орнату пакетін жасау үшін Kaspersky дерекқорынан бағдарламаны таңдау**. Орнату пакетін жасауды қажет ететін Kaspersky дерекқорынан үшінші тарап бағдарламасын таңдағыңыз келсе, осы нұсқаны таңдаңыз. Дерекқоры Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын іске қосу кезінде автоматты түрде жасалады; бағдарламалар тізімде көрсетіледі.

- **Орнату пакетін операциялық жүйенің кескінімен бірге жасау**. Эталондық құрылғының операциялық жүйесінің кескіні бар орнату пакетін жасағыңыз келсе, осы нұсқаны таңдаңыз.

  Шебердің жұмысы нәтижесінде Басқару серверінің **Анықтамалық құрылғының ОЖ кескінінің орнату пакетін жасау** атты тапсырмасы жасалады. Бұл тапсырманы орындау нәтижесінде PXE серверін немесе қашықтан орнату тапсырмасын пайдаланып операциялық жүйенің кескінін орналастыру үшін пайдалануға болатын орнату пакеті жасалады.

4. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысының нәтижесінде бағдарламаны клиент құрылғыларына орнату үшін пайдалануға болатын орнату пакеті жасалады. Сіз орнату пакетін консоль ағашының **Орнату пакеттері** қалтасында қарай аласыз.

Бағдарламалардың орнату пакеттері үшін сертификатты шығару

Бағдарламаның орнату пакетіне сертификатты шығару үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.

   Қашықтан орнату қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. **Орнату пакеттері** қалтасының контекстік мәзірінен **Кеңейтілген** тармағын таңдаңыз.

   Нәтижесінде, **Орнату пакеттері** қалтасы сипаттары терезесі ашылады.

3. **Орнату пакеттері** қалтасы сипаттары терезесінен **Автономды пакеттердің қолтаңбасы** бөлімін таңдаңыз.

4. **Автономды пакеттердің қолтаңбасы** бөлімінде **Белгілеу** түймесін басыңыз.

   Сертификат терезесі ашылады.

5. **Сертификат түрі** өрісінде сертификаттың жалпыға ортақ немесе жеке түрін таңдаңыз:

   - **PKCS #12 контейнері** мәні таңдалған болса, сертификат файлы мен құпиясөзді көрсетіңіз.
   - **X.509 сертификаты** мәні таңдалған болса:

     a. жеке кілт файлын (prk немесе pem кеңейтімі бар файл) көрсетіңіз;

     b. жеке кілт құпиясөзін көрсетіңіз;

     c. жалпыға ортақ кілт файлын (cer кеңейтімі бар файл) көрсетіңіз.

6. **OK** түймесін басыңыз.

Нәтижесінде, бағдарламаның орнату пакеті үшін сертификат шығарылады.

Клиент құрылғыларына бағдарламаларды орнату

Клиент құрылғыларына бағдарламаны орнату үшін:

1. Қорғанысты орналастыру шеберін іске қосу үшін консоль ағашында **Қашықтан орнату** қалтасын ашып, **Орнату пакетін басқарылатын құрылғыларда (жұмыс станциялары) орналастыру** сілтемесінен өтіңіз.
2. Шебердің **Орнату пакетін таңдау** терезесінде орнатқыңыз келетін бағдарламаның орнату пакетін көрсетіңіз.
3. Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысының нәтижесінде клиент құрылғыларында бағдарламаны қашықтан орнату тапсырмасы жасалады. Тапсырманы **Тапсырмалар** қалтасында іске қосуға немесе тоқтатуға болады.

Желілік агентті Windows, Linux және macOS операциялық жүйелері бар клиент құрылғыларына қорғанысты орналастыру шебері арқылы орнатуға болады.

Linux операциялық жүйелері бар құрылғыларда Kaspersky Security Center көмегімен 64 разрядты қауіпсіздік бағдарламаларын басқару үшін Linux үшін 64 разрядты Желілік агентті пайдалану қажет. Желілік агенттің қажетті нұсқасын Техникалық қолдау қызметі веб-сайтынан жүктеп алуға болады.

Linux операциялық жүйесі бар құрылғыға қашықтан Желілік агентті орнатпас бұрын құрылғыны дайындау керек.

Нысанды тексерумен жұмыс

Бұл бөлімде нысандарды тексерумен жұмыс істеу туралы ақпарат бар. Kaspersky Security Center нысандардың өзгерістерін бақылауға мүмкіндік береді. Нысанның өзгерістерін сақтаған сайын, *тексеру* жасалады. Әр тексерудің өзі нөмірі бар.

Тексерулермен жұмысты қолдайтын бағдарлама нысандары:

- Басқару серверінің қасиеттері
- Саясаттар
- Тапсырмалар
- Басқару топтары
- Пайдаланушы есептік жазбалары
- Орнату пакеттері

Нысандарды тексерумен келесі әрекеттерді орындауыңызға болады:

- таңдалған тексеруді ағымдағы тексерумен салыстыру;
- таңдалған тексерулерді салыстыру;
- нысанды басқа бір типті нысанның таңдалған тексеруімен салыстыру;
- таңдалған тексеруді қарап шығу;
- нысанның өзгерістерін таңдалған тексеруге шегіндіру;
- тексерулерді TXT файлына сақтау.

Тексерулермен жұмыс істеуді қолдайтын нысандардың сипаттары терезесінде **Тексерістер журналы** бөлімінде келесі ақпаратпен бірге нысанды тексеру тізімі көрсетіледі:

- нысанды тексеру нөмірі;
- нысанды өзгерту күні мен уақыты;
- нысанды өзгерткен пайдаланушы атауы;
- нысанмен орындалған әрекет;
- нысан параметрлерінің өзгерістерін тексеру сипаттамасы.

Нысандарды тексеру туралы

Нысандарды тексерумен келесі әрекеттерді орындауыңызға болады:

- таңдалған тексеруді ағымдағы тексерумен салыстыру;
- таңдалған тексерулерді салыстыру;
- нысанды басқа бір типті нысанның таңдалған тексеруімен салыстыру;
- таңдалған тексеруді қарап шығу;

- нысанның өзгерістерін таңдалған тексеруге шегіндіру;
- тексерулерді TXT файлына сақтау.

Тексерулермен жұмыс істеуді қолдайтын нысандардың сипаттары терезесінде **Тексерістер журналы** бөлімінде келесі ақпаратпен бірге нысанды тексеру тізімі көрсетіледі:

- нысанды тексеру нөмірі;
- нысанды өзгерту күні мен уақыты;
- нысанды өзгерткен пайдаланушы атауы;
- нысанмен орындалған әрекет;
- нысан параметрлерінің өзгерістерін тексеру сипаттамасы.

Тексерістер журналы бөлімін қарап шығу

Нысанның тексерулерін ағымдағы тексерумен салыстыра аласыз, тізімде таңдалған тексерулерді салыстыра аласыз немесе нысанды тексерулерді басқа бір типті нысанның тексерулерімен салыстыра аласыз.

*Нысанның **Тексерістер журналы** бөлімін қарап шығу үшін:*

1. Консоль ағашында нысандардың бірін таңдаңыз:
   - **Басқару сервері** түйіні;
   - **Саясаттар** қалтасы;
   - **Тапсырмалар** қалтасы;
   - басқару тобы қалтасы;
   - **Пайдаланушылардың есептік жазбалары** қалтасы;
   - **Жойылған нысандар** қалтасы;
   - **Қашықтан орнату** салынған **Орнату пакеттері** ішкі қалтасы.
2. Тиісті нысанның орналасқан жеріне байланысты келесі әрекеттердің бірін орындаңыз:
   - Нысан **Басқару сервері** түйінінде немесе басқару тобы қалтасында болса, нысанның мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
   - Нысан **Саясаттар**, **Тапсырмалар**, **Пайдаланушылардың есептік жазбалары**, **Жойылған нысандар** немесе **Орнату пакеттері** қалтасында болса, қалтаны таңдап, тиісті жұмыс аймағында нысанды таңдаңыз.

   Нысан сипаттары терезесі ашылады.
3. **Бөлімдер** тақтасында **Тексерістер журналы** бөлімін таңдаңыз.

   Тексерулер тарихы жұмыс аймағында көрсетіледі.

Нысанды тексерулерді салыстыру

Нысанның алдыңғы тексерулерін ағымдағы тексерумен салыстыра аласыз, тізімде таңдалған тексерулерді салыстыра аласыз немесе нысанды тексерулерді басқа бір типті нысанның тексерулерімен салыстыра аласыз.

Нысанды тексерулерді салыстыру үшін:

1. Нысанды таңдап, сол нысанның сипаттар терезесіне өтіңіз.
2. Тапсырма сипаттары терезесінде **Тексерістер журналы** бөлімін таңдаңыз.
3. Нысанды тексеру тізіміндегі жұмыс аймағында салыстыру үшін тексеруді таңдаңыз.

   Екіден артық нысан тексерулерін таңдау үшін **SHIFT** және **CTRL** пернелерін қолданыңыз.
4. Келесі әрекеттердің бірін орындаңыз:

   - **Салыстыру** түймесін басып, ашылмалы тізімнен келесі мәндердің бірін таңдаңыз:

     - **Ағымдағы тексерумен салыстыру**

       Таңдалған тексеруді ағымдағы нұсқамен салыстыру үшін осы нұсқаны таңдаңыз.

     - **Таңдалған тексерулерді салыстыру**

       Екі таңдалған тексеруді салыстыру үшін осы нұсқаны таңдаңыз.

     - **Басқа тапсырмамен салыстыру**

       Тапсырмаларды тексерулермен жұмыс істегенде, таңдалған тексеруді басқа тапсырманы тексерумен салыстыру үшін **Басқа тапсырмамен салыстыру** нұсқасын таңдаңыз.

       Саясаттарды тексерулермен жұмыс істеу кезінде, таңдалған тексеруді басқа саясатты тексерумен салыстыру үшін **Басқа саясатпен салыстыру** нұсқасын таңдаңыз.

   - Тексеру атауын екі рет басыңыз, содан кейін ашылатын тексеру сипаттары терезесіндегі келесі түймелердің бірін басыңыз:

     - **Ағымдағымен салыстыру**

       Таңдалған тексеруді ағымдағы тексерумен салыстыру үшін осы түймені басыңыз.

     - **Алдыңғымен салыстыру**

       Таңдалған тексеруді алдыңғы нұсқасымен салыстыру үшін осы түймені басыңыз.

HTML пішіміндегі тексерулерді салыстыру есебі, сіздің әдепкі бойынша шолғышыңызда көрсетіледі.

Есепте тексеру параметрлерінің кейбір блоктарын азайтуға болады. Тексеру параметрлері блогын азайту үшін блоктың атауы жанындағы көрсеткі белгішесін (▲) басыңыз.

Басқару серверін тексеру келесі салалардағы ақпараттан басқа, өзгерістер туралы ақпаратты қамтиды:

- **Трафик** бөлімі;
- **Тегтерді белгілеу ережелері** бөлімі;
- **Хабарландыру** бөлімі;
- **Тарату нүктелері** бөлімі;
- **Вирустық шабуыл** бөлімі.

  Вирустық шабуыл бөлімінен Вирустық шабуыл оқиғасы бойынша саясаттарды белсендіруді конфигурациялау туралы ақпарат жазылмайды.

Жойылған нысанды тексеруді қолданыстағы нысанды тексерумен салыстыра аласыз, бірақ керісінше емес: қолданыстағы нысанды тексеруді жойылған нысанды тексерумен салыстыра алмайсыз.

Нысанды тексерулерді және жойылған нысандар туралы ақпаратты сақтау мерзімін белгілеу

Нысанды тексерулерді сақтау мерзімі жойылған нысандар туралы ақпаратты сақтау мерзімімен бірдей. Әдепкі бойынша белгіленген мерзім – 90 күн. Бұл, бағдарлама аудитін үнемі жүргізіп отыру үшін жеткілікті.

Тек **Жойылған нысандар** аймағында **Өзгерту** құқықтары бар пайдаланушылар ғана нысанды тексерулерді және жойылған нысандар туралы ақпаратты сақтау мерзімін өзгерте алады.

Нысанды тексерулерді және жойылған нысандар туралы ақпаратты сақтау мерзімін өзгерту үшін:

1. Консоль ағашында, нысанды тексерулерді және жойылған нысандар туралы ақпаратты сақтау мерзімін өзгерту қажет болған Басқару серверін таңдаңыз.
2. Нысанның контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде, **Тексерістер журналының қоймасы** бөлімінде қажетті сақтау мерзімін көрсетіңіз (күндерде).
4. **ОК** түймесін басыңыз.

Нысанның тексерулері және жойылған нысандар туралы ақпарат көрсетілген күн бойы сақталады.

Нысанды тексеруді қарау

Егер сізге белгілі бір кезеңде нысанмен қандай өзгерістер болғанын білу қажет болса, сіз нысанды тексеруді қарап шыға аласыз.

Нысанды тексеруді қарау үшін:

1. Нысанның **Тексерістер журналы** бөліміне өтіңіз.
2. Нысанды тексеру тізімінен параметрлерін қарау керек болған тексеруді таңдаңыз.

3. Келесі әрекеттердің бірін орындаңыз:

   - **Тексерісті көру** түймесін басыңыз.
   - Тексеру сипаттары терезесін ашу үшін тексеру атауын екі рет басып, **Тексерісті көру** түймесін басыңыз.

   HTML пішімінде таңдалған нысанды тексеру параметрлері бар есеп көрсетіледі. Есепте нысанды тексеру параметрлерінің кейбір блоктарын азайтуға болады. Тексеру параметрлері блогын азайту үшін блоктың атауы жанындағы көрсеткі белгішесін (▲) басыңыз.

Нысанды тексеруді файлда сақтау

Нысанды тексеруді мәтіндік файлға сақтауға болады, мысалы, файлды электрондық пошта арқылы жіберу үшін.

Нысанды тексеруді файлда сақтау үшін:

1. Нысанның **Тексерістер журналы** бөліміне өтіңіз.
2. Нысанды тексеру тізімінен параметрлерін сақтау керек болған тексеруді таңдаңыз.
3. **Кеңейтілген** түймесін басыңыз да, ашылатын тізімнен **Файлға сақтау** мәнін таңдаңыз.

   Тексеру TXT файлына сақталады.

Өзгерістерді шегіндіру

Қажет болса, нысанның өзгерістерін шегіндіруге болады. Мысалы, саясат параметрлерін белгілі бір күндегі күйге кері қайтару қажет болып қалуы мүмкін.

Нысан өзгерістерін шегіндіру үшін:

1. Нысанның **Тексерістер журналы** бөліміне өтіңіз.
2. Нысанды тексеру тізімінде, өзгерістерін шегіндіру қажет болған тексеру нөмірін таңдаңыз.
3. **Кеңейтілген** түймесін басыңыз да, ашылатын тізімнен **Шегіндіру** мәнін таңдаңыз.

   Таңдалған тексеруге шегіндіру орын алады. Нысанды тексеру тізімінде орындалған әрекет туралы жазба көрсетіледі. Тексеру сипаттамасында, нысанды қайтарған тексеру нөмірі туралы ақпарат көрсетіледі.

Тексерудің сипаттамасын қосу

Алдағыда тізімде қажетті тексеруді оңай тауып алу үшін тексеру сипаттамасын қосуға болады.

Тексеру сипаттамасын қосу үшін:

1. Нысанның **Тексерістер журналы** бөліміне өтіңіз.
2. Нысанды тексеру тізімінде, сипаттамасын қосу қажет болған тексеруді таңдаңыз.

3. **Сипаттама** түймесін басыңыз.
4. **Нысанды тексерудің сипаттамасы** терезесінде тексеру сипаттамасы мәтінін енгізіңіз.

   Әдепкі бойынша, нысанды тексеру сипаттамасы толтырылмаған.
5. **ОК** түймесін басыңыз.

Нысандарды жою

Бұл бөлімде нысандарды жою туралы ақпарат берілген.

Сіз келесі нысандарды жоя аласыз:

- Саясаттар
- Тапсырмалар
- Орнату пакеттері
- Виртуалды Басқару серверлері
- Пайдаланушылар
- Қауіпсіздік топтары
- Басқару топтары

Нысанды жою үшін:

1. Kaspersky Security Center Web Console қажетті бөлімін ашып, нысанды таңдаңыз.
2. Құралдар тақтасындағы **Жою** түймесін басыңыз.
3. Пайда болған терезеде таңдауыңызды растау үшін **ОК** түймесін басыңыз.

   Таңдалған нысан жойылды.

Сіз нысанды жойған кезде, бұл туралы ақпарат дерекқорға жазылады. Жойылған нысандардың ақпаратын сақтау мерзімі, нысанды тексеруді сақтау мерзімімен бірдей (ұсынылатын мерзімі 90 күн). Құқықтардың **Жойылған нысандар** аймағында **Өзгерту** рұқсатыңыз болса ғана, сақтау орнының шартын өзгертуге болады.

Клиенттік құрылғыларды жою туралы

Басқарылатын құрылғы басқару тобынан жойылғанда, бағдарлама құрылғыны Тағайындалмаған құрылғылар тобына жылжытады. Құрылғы жойылғаннан кейін, Kaspersky орнатылған қолданбалары – Желілік агент және Kaspersky Endpoint Security сияқты қауіпсіздік бағдарламасы құрылғыда қалады.

Kaspersky Security Center келесі ережелерге сәйкес Тағайындалмаған құрылғылар тобындағы құрылғыларды өңдейді:

- Құрылғыны жылжыту ережелерін конфигурациялаған болсаңыз және құрылғы жылжыту ережесінің шарттарына сай болса, құрылғы ережеге сәйкес автоматты түрде басқару тобына жылжытылады.

- Құрылғы Тағайындалмаған құрылғылар тобында сақталады және құрылғыны сақтау ережелеріне сәйкес топтан автоматты түрде жойылады.

  Құрылғыны сақтау ережелері, бір немесе бірнеше дискілері толық дискілік шифрлау арқылы шифрланған құрылғыларға әсер етпейді. Мұндай құрылғылар автоматты түрде жойылмайды – оларды тек қолмен жоюға болады. Шифрланған қатты дискісі бар құрылғыны жою қажет болса, алдымен дискінің шифрын шешіп, содан кейін құрылғыны алып тастаңыз.

  > Шифрланған қатты дискісі бар құрылғыны алып тастаған кезде, дискінің шифрын шешуге қажетті деректер де жойылады. Егер сіз осындай құрылғыларды (**Тағайындалмаған құрылғылар** тобынан немесе **Басқарылатын құрылғылар** тобынан) жойған кезде ашылатын растау терезесінде **Тәуекелді түсінемін және таңдалған құрылғыларды жойғым келеді** құсбелгісін қойсаңыз, бұл сіздің деректердің кейінірек жойылатынын білетініңізді білдіреді.

  Бұл жағдайда, дискінің шифрын ашу үшін келесі шарттар орындалуы керек:

  - Дискінің шифрын шешуге қажетті деректерді қалпына келтіру үшін құрылғы Басқару серверіне қайта қосылады.
  - Құрылғының пайдаланушысы шифрды шешу құпиясөзін есте сақтайды.
  - Құрылғыда Kaspersky Endpoint Security for Windows сияқты дискіні шифрлау үшін пайдаланылған қауіпсіздік бағдарламасы орнатылған.

  Егер диск Kaspersky Disk Encryption технологиясы арқылы шифрланған болса, FDERT Restore утилитасын пайдаланып деректерді қалпына келтіруге де болады.

> VDI жүйесінде шифрланған дискілері бар құрылғы болса, құрылғыны жойғаннан кейін шифрланған дискідегі ақпарат жойылады.

Құрылғыны Тағайындалмаған құрылғылар тобынан қолмен жойған кезде, бағдарлама құрылғыны тізімнен жояды. Құрылғы жойылғаннан кейін, Kaspersky орнатылған бағдарламалары (бар болса) құрылғыда қалады. Содан кейін, құрылғы әлі де Басқару серверіне көрініп тұрса және сіз тұрақты желі сұрауын конфигурациялаған болсаңыз, Kaspersky Security Center Linux желі сауалнамалары кезінде құрылғыны анықтайды және оны Тағайындалмаған құрылғылар тобына қайта қосады. Сондықтан, егер ол Басқару серверіне көрінбейтін болса ғана құрылғыны қолмен алып тастаған жөн.

Нысанды жою

Негізгі функционалдылық санатында өзгерту құқығыңыз болса, саясаттар, тапсырмалар, орнату пакеттері, ішкі пайдаланушылар және ішкі қауіпсіздік топтары сияқты нысандарды жоя аласыз (толық ақпарат алу үшін Пайдаланушылар және пайдаланушы топтарына құқықтар тағайындау мақаласын қараңыз).

Қашықтан орнату тапсырмаларында пайдаланылатын орнату қалталарын жоя алмайсыз. Алдымен сәйкес тапсырмаларды тоқтату керек. Басқару тобындағы автоматты орнату тапсырмалары туралы қосымша ақпаратты Қолданбаларды басқару тобының құрылғыларына автоматты түрде орнату мақаласынан қараңыз.

Нысанды жою үшін:

1. Консоль ағашының қажетті қалтасының жұмыс аймағында нысанды таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:
   - Нысанның контекстік мәзірінде **Жою** тармағын таңдаңыз.
   - **DELETE** түймесін басыңыз.

Нысан жойылады, ал бұл туралы ақпарат дерекқорға жазылады.

Жойылған нысандар туралы ақпаратты қарау

Жойылған нысандар туралы ақпарат **Жойылған нысандар** қалтасында нысанды тексерумен бірдей мерзім бойы сақталады (ұсынылатын мерзімі 90 күн).

Жойылған нысандар аймағына арналған **Оқу** құқықтары бар пайдаланушылар ғана жойылған нысандар тізімін қарай алады (толығырақ ақпарат Пайдаланушылар және пайдаланушы топтарына құқықтар тағайындау бөлімінен қараңыз).

Жойылған нысандар тізімін қарау үшін,

Консольдер ағашында **Жойылған нысандар** тармағын таңдаңыз (әдепкі бойынша **Жойылған нысандар** қалтасы **Кеңейтілген** қалтасына салынған).

Жойылған нысандар аймағы үшін оқу құқықтарыңыз болмаса, **Жойылған нысандар** қалтасында бос тізім көрсетіледі.

Жойылған нысандар қалтасының жұмыс аймағында жойылған нысандар туралы келесі ақпарат бар:

- **Атауы**. Жойылған нысанның атауы.
- **Түрі**. Саясат, тапсырма немесе орнату пакеті сияқты нысан түрі.
- **Уақыт**. Нысан жойылған уақыт.
- **Пайдаланушы**. Нысан жойған пайдаланушының есептік жазбасы.

Жойылған нысан туралы көбірек ақпаратты қарау үшін:

1. Консольдер ағашында **Жойылған нысандар** тармағын таңдаңыз (әдепкі бойынша **Жойылған нысандар** қалтасы **Кеңейтілген** қалтасына салынған).
2. **Жойылған нысандар** қалтасының жұмыс аймағында қажетті нысанды таңдаңыз.

   Жұмыс аймағының оң жағында таңдалған нысанмен жұмыс істеуге арналған өріс көрсетіледі.
3. Келесі әрекеттердің бірін орындаңыз:

   - Таңдалған нысанмен жұмыс істеу блогында **Сипаттар** сілтемесінен өтіңіз.
   - Нысанның контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Нысан сипаттары терезесі ашылып, онда келесі ақпарат көрсетіледі:

   - **Жалпы**
   - **Тексерістер журналы**

Нысандарды жойылған нысандар тізімінен жою

Жойылған нысандар аймағына арналған **Өзгерту** құқықтары бар пайдаланушылар ғана жойылған нысандар тізімінен нысандарды жоя алады (толығырақ ақпарат Пайдаланушылар және пайдаланушы топтарына құқықтар тағайындау бөлімінен қараңыз).

Нысанды жойылған нысандар тізімінен жою үшін:

1. Консоль ағашында қажетті Басқару серверінің түйінін таңдап, **Жойылған нысандар** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында, жойғыңыз келетін нысанды немесе нысандарды таңдаңыз.
3. Келесі әрекеттердің бірін орындаңыз:

   - **DELETE** түймесін басыңыз.
   - Сіз таңдаған нысанның немесе нысандардың контекстік мәзірінен **Жою** тармағын таңдаңыз.
4. Диалогтық терезеде **Иә** түймесін басыңыз.

Нысан жойылған нысандар тізімінен жойылды. Нысанның барлық ақпараты (барлық тексерулерді қоса алғанда) дерекқордан жойылды. Сіз бұл ақпаратты қалпына келтіре алмайсыз.

Ұялы құрылғыларды басқару

Kaspersky Security Center арқылы ұялы құрылғылардың қорғанысын басқару Ұялы құрылғыларды басқару құрамдасы арқылы жүзеге асырылады. Егер сіз ұйым қызметкерлеріне тиесілі ұялы құрылғыларды басқаруды жоспарласаңыз, Ұялы құрылғыларды басқаруды қосуыңыз керек.

Бұл бөлімде Ұялы құрылғыларды басқаруды қосу, конфигурациялау және өшіру туралы нұсқаулар берілген. Сондай-ақ, бұл бөлімде Басқару серверіне қосылған ұялы құрылғыларды басқару сипатталған.

Kaspersky Security for Mobile туралы толығырақ ақпаратты *Kaspersky Security for Mobile анықтамасынан* қараңыз.

Сценарий: Ұялы құрылғыларды басқаруды орналастыру

Бұл бөлімде Kaspersky Security Center бағдарламасында Ұялы құрылғыларды басқару мүмкіндіктерін конфигурациялауға арналған сценарий келтірілген.

Алдын ала талаптар

Лицензияңыз Ұялы құрылғыларды басқару мүмкіндіктеріне қол жеткізуге мүмкіндік беретініне көз жеткізіңіз.

Кезеңдер

Ұялы құрылғыларды басқару мүмкіндіктерін қолдану келесі кезеңдерден тұрады:

1. **Порттарды дайындау**

   Басқару серверінде 13292-порт бар екеніне көз жеткізіңіз. Бұл порт ұялы құрылғыларды қосу үшін қажет. Сондай-ақ, сіз 17100-портты қолжетімді ете аласыз. Бұл порт тек басқарылатын ұялы құрылғылар үшін прокси-серверді іске қосу үшін қажет; егер басқарылатын ұялы құрылғылар интернетке қатынаса алса, бұл портты қолжетімді ету қажет емес.

2. **Ұялы құрылғыларды басқаруды қосу**

   Басқару серверін жылдам іске қосу шеберін іске қосу кезінде немесе кейінірек Ұялы құрылғыларды басқаруды қосуға болады.

3. **Басқару серверінің сыртқы мекенжайын көрсету**

   Басқару серверін жылдам іске қосу шеберін іске қосу кезінде немесе кейінірек сыртқы мекенжайды көрсетуге болады. Егер сіз орнату үшін Ұялы құрылғыларды басқаруды таңдамасаңыз және бағдарламаны орнату шеберінде мекенжайды көрсетпесеңіз, орнату пакетінің сипаттарында сыртқы мекенжайды көрсетіңіз.

4. **Ұялы құрылғыларды Басқарылатын құрылғылар тобына қосу**

   Ұялы құрылғыны Басқарылатын құрылғылар тобына қосып, осылайша оларды саясаттардың көмегімен басқарыңыз. Басқару серверін жылдам іске қосу шебері қадамдарының бірінде жылжыту ережесін жасай аласыз. Сондай-ақ, жылжыту ережесін кейінірек жасай аласыз. Егер сіз мұндай ережені жасамасаңыз, ұялы құрылғыларды Басқарылатын құрылғылар тобына қолмен қоса аласыз.

   Ұялы құрылғыларды Басқарылатын құрылғылар тобына тікелей қоса аласыз немесе олар үшін ішкі топты (немесе бірнеше ішкі топты) жасай аласыз.

   Кейінірек, кез келген уақытта жаңа ұялы құрылғыны Басқару серверіне ұялы құрылғыны қосу шебері арқылы қосуға болады.

5. **Ұялы құрылғылар үшін саясат құру**

   Ұялы құрылғыларды басқару үшін, олар тиесілі болып саналатын осы құрылғылар үшін саясатты (немесе бірнеше саясатты) жасаңыз. Сіз саясаттың параметрлерін кез келген уақытта өзгерте аласыз.

Нәтижелер

Сценарий аяқталғаннан кейін, сіз Kaspersky Security Center бағдарламасын қолдана отырып, Android және iOS құрылғыларын басқара аласыз. Сіз ұялы құрылғылардың сертификаттарымен жұмыс істей аласыз және ұялы құрылғыларға пәрмендерді жібере аласыз.

iOS MDM құрылғыларын басқаруға арналған топтық саясаттар туралы

iOS MDM құрылғыларын басқару үшін сіз Kaspersky Security Center бағдарламасының жеткізу жиынтығына кіретін Kaspersky Device Management for iOS басқару плагинін қолдана аласыз. Kaspersky Device Management for iOS басқару плагині, iPhone Configuration Utility пайдаланбай, iOS MDM құрылғыларының конфигурациялық параметрлерін конфигурациялау үшін топтық саясаттарды жасауға мүмкіндік береді.

iOS MDM құрылғыларын басқаруға арналған топтық саясаттар әкімшіге келесі мүмкіндіктер береді:

- құрылғыда құпиясөзді қолданудың қауіпсіздік параметрлерін конфигурациялау;
- құрылғының аппараттық функцияларын қолдануға қойылатын шектеулерді, сондай-ақ ұялы құрылғыларды орнатуға, жоюға қойылатын шектеулерді конфигурациялау;
- құрылғыда кіріктірілген ұялы қолданбаларды, мысалы, YouTube™, iTunes Store немесе Safari қолдану үшін шектеулерді конфигурациялау;
- құрылғының орналасқан өңірі бойынша медиаконтентті (мысалы, фильмдер және тв-шоу) қарауға қойылатын шектеулерді конфигурациялау;
- құрылғыны интернетке прокси-сервер арқылы қосу параметрлерін конфигурациялау (Глобалды HTTP-прокси);
- пайдаланушы корпоративтік бағдарламалар мен сервистерге қатынасу мүмкіндігіне ие бола алатын (бірыңғай кіру) бірыңғай есептік жазба параметрлерін конфигурациялау;
- ұялы құрылғыларда интернеттің қолданылуын бақылау (веб-сайттарға кіру);
- әртүрлі түпнұсқалық растама тетіктері мен желілік протоколдарды қолдану арқылы сымсыз желілердің (Wi-Fi), қатынасу нүктелерінің (APN), виртуалды жеке желілердің (VPN) параметрлерін конфигурациялау;
- фотосуреттер, музыка және бейнені ағынмен жіберу үшін AirPlay құрылғыларына қосылу параметрлерін конфигурациялау;
- құрылғыдағы құжаттарды сымсыз тәсілмен басып шығару үшін AirPrint™ принтерлеріне қосылу параметрлерін конфигурациялау;
- Microsoft Exchange серверімен синхрондау параметрлерін, сондай-ақ құрылғыларда корпоративтік поштаны қолдану үшін пайдаланушылардың есептік жазбаларын конфигурациялау;
- LDAP каталогтар қызметімен синхрондау үшін пайдаланушының есептік жазбаларын конфигурациялау;
- CalDAV және CardDAV сервистеріне қосылу үшін пайдаланушының есептік жазбаларын конфигурациялау, соның арқасында пайдаланушы корпоративтік күнтізбелер мен контактілер тізімін пайдалана алады;

- пайдаланушы құрылғысында iOS интерфейсінің параметрлерін конфигурациялау, мысалы, таңдаулы веб-сайттарға арналған қаріптер немесе белгішелер;
- құрылғыға жаңа қауіпсіздік сертификаттарын қосу;
- құрылғының Сертификаттау орталығынан сертификаттарды автоматты түрде алуы үшін SCEP сервері (Simple Certificate Enrollment Protocol) параметрлерін конфигурациялау;
- ұялы қолданбалардың жұмыс істеуі үшін өзіндік параметрлерді қосу.

iOS MDM құрылғысын басқару саясаты, iOS MDM серверін (бұдан әрі «Ұялы құрылғылар сервері» деп аталады) қамтитын басқару тобына тағайындалуымен ерекшеленеді. Осы саясатта белгіленген барлық параметрлер, алдымен Ұялы құрылғылар серверіне, содан кейін сол сервер басқаратын ұялы құрылғыларға таратылады. Басқару топтарының иерархиялық құрылымын қолданған жағдайда, ұялы құрылғылардың қосалқы серверлері ұялы құрылғылардың басты серверлерінен саясат параметрлерін алады және оларды ұялы құрылғыларға таратады.

Kaspersky Security Center Басқару консолі арқылы iOS MDM құрылғыларын басқару үшін топтық саясатты пайдалану туралы қосымша ақпаратты *Kaspersky Security for Mobile* анықтамасынан қараңыз.

Ұялы құрылғыларды басқаруды қосу

Ұялы құрылғыларды басқаруды үшін Ұялы құрылғыларды басқаруды қосу керек. Бағдарламаны жылдам іске қосу шеберінде Ұялы құрылғыларды басқаруды қоспасаңыз, мұны кейінірек жасай аласыз. Ұялы құрылғыларды басқару үшін лицензия керек.

Ұялы құрылғыларды басқаруды қосу тек негізгі Басқару серверінде ғана қолжетімді.

Ұялы құрылғыларды басқаруды қосу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағындағы **Мобильді құрылғыларды басқаруды қосу** түймесі арқылы тапсырманы жасау шеберін іске қосыңыз. Бұл түйме, бұған дейін **Мобильді құрылғыларды басқару** қоспаған болсаңыз ғана қолжетімді.

   Басқару серверін жылдам іске қосу шеберінің **Қосымша құрамдастар** терезесі көрсетіледі.
3. Ұялы құрылғыларды басқару үшін **Мобильді құрылғыларды басқаруды қосу** тармағын таңдаңыз.
4. **Бағдарламаны белсендіру әдісін таңдау** терезесінде кілт файлы немесе белсендіру коды арқылы бағдарламаны белсендіріңіз.

   Ұялы құрылғыларды басқару мүмкіндігін белсендірмейінше, Ұялы құрылғыларды басқару қолжетімді болмайды.
5. Интернетке қосылу үшін прокси-серверді пайдаланғыңыз келсе, **Прокси-сервердің интернет желісін пайдалану рұқсатын алу параметрлері** бетінде **Прокси-серверді пайдалану** жалаушасын қойыңыз. Жалауша қойылса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылу параметрлерін конфигурациялаңыз.

6. **Плагиндердің және орнату пакеттерінің жаңартуларын тексеру** бетінде келесі нұсқалардың бірін таңдаңыз:

   - **Плагиндердің және орнату пакеттерінің жаңартылғанын тексеру**

     Өзектілігін тексеруді іске қосу. Тексеру плагиндердің немесе орнату пакеттерінің ескірген нұсқаларын қолдануды анықтаса, шебер ескірген нұсқалардың орнына өзекті нұсқаларды жүктеуді ұсынады.

   - **Тексеруді өткізіп жіберу**

     Плагиндер мен орнату пакеттерінің өзектілігін тексермей, жұмысты жалғастыру. Бұл нұсқаны, мысалы, сізде интернетке қатынасу мүмкіндігі болмаса немесе қандай да бір себептермен бағдарламаның ескірген нұсқасын пайдалануды жалғастырғыңыз келсе таңдай аласыз.

     > Плагиндердің өзектілігін тексеруді өткізіп жіберу бағдарламаның дұрыс жұмыс істемеуіне әкелуі мүмкін.

7. **Плагиндердің қолжетімді соңғы нұсқалары** терезесінде плагиндердің қажетті тілдегі соңғы нұсқаларын жүктеп алыңыз және орнатыңыз. Плагинді жаңарту үшін лицензия қажет емес.

   Плагиндер мен пакеттерді орнатқаннан кейін, бағдарлама ұялы құрылғылардың дұрыс жұмыс істеуі үшін барлық қажетті плагиндердің орнатылғанын тексереді. Плагиндердің ескірген нұсқалары табылса, шебер ескірген нұсқалардың орнына өзекті нұсқаларды жүктеуді ұсынады.

8. **Ұялы құрылғыларды қосу параметрлері** бетінде Басқару серверінің порттарын конфигурациялаңыз.

Шебердің жұмысы аяқталғаннан кейін келесі өзгерістер орындалады:

- Kaspersky Endpoint Security for Android саясаты жасалды;
- Kaspersky Device Management for iOS саясаты жасалды;
- ұялы құрылғыларға арналған Басқару сервері порттары ашық.

Ұялы құрылғыларды басқару параметрлерін өзгерту

Ұялы құрылғыларды қолдауды қосу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында **Ұялы құрылғыларға арналған қосылым порттары** сілтемесі бойынша өтіңіз.

   Басқару серверінің сипаттары терезесінің **Қосымша порттар** бөлімі көрсетіледі.
3. **Қосымша порттар** бөлімінде өзіңізге қажетті параметрлерді өзгертіңіз:

   - Белсендіру прокси-серверіне арналған SSL порты
   - **Ұялы құрылғыларға арналған портты ашу**

     Ұялы құрылғылар Лицензиялау серверіне қосылатын порт ашылады. Төмендегі өрістерде порт нөмірін және басқа конфигурацияларды белгілеуге болады.

     Әдепкі бойынша, параметр қосулы.

- **Ұялы құрылғыны синхрондау порты**

  Ұялы құрылғылар Басқару серверіне қосылып, онымен ақпарат алмасатын порт нөмірі. Әдепкі бойынша 13292-порт орнатылған.

  13292-порт қандай да бір басқа мақсаттарда пайдаланылса, басқа портты тағайындауға болады.

- **Ұялы құрылғыларды белсендіруге арналған порт**

  Kaspersky Endpoint Security for Android қолданбасын Kaspersky белсендіру серверлеріне қосу порттары.

  Әдепкі бойынша 17100-порт орнатылған.

4. **OK** түймесін басыңыз.

Ұялы құрылғыларды басқаруды өшіру

Ұялы құрылғыларды басқаруды өшіру тек негізгі Басқару серверінде ғана қолжетімді.

Ұялы құрылғыларды басқаруды өшіру үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағында **Қосымша компоненттерді конфигурациялау** сілтемесі бойынша өтіңіз.

   Басқару серверін жылдам іске қосу шеберінің **Қосымша құрамдастар** терезесі көрсетіледі.
3. Ұялы құрылғыларды енді басқарғыңыз келмесе, **Ұялы құрылғыларды басқару мүмкіндігін қоспау** тармағын таңдаңыз.
4. **OK** түймесін басыңыз.

Бұған дейін қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды. Ұялы құрылғыларды қосу порты мен ұялы құрылғыларды белсендіру порты автоматты түрде жабылады.

Kaspersky Endpoint Security for Android және Kaspersky Device Management for iOS жасалған саясаттары жойылмайды. Сертификаттарды шығару ережелері өзгермейді. Орнатылған плагиндер жойылмайды. Ұялы құрылғыларды жылжыту ережесі жойылмайды.

Ұялы құрылғыларды басқаруды қайта қосқаннан кейін, басқарылатын ұялы құрылғыларда ұялы құрылғыларды басқаруға қажетті ұялы қолданбаларды қайта орнату қажет болуы мүмкін.

Ұялы құрылғыларға арналған пәрмендермен жұмыс істеу

Бұл бөлімде Kaspersky Security Center қолдау көрсететін мобильдік құрылғыларды басқаруға арналған пәрмендер туралы ақпарат берілген. Бөлімде пәрмендерді ұялы құрылғыларға жіберу, сондай-ақ пәрмендер журналында пәрмендердің орындалу күйін көру бойынша нұсқаулар берілген.

Ұялы құрылғыларды басқаруға арналған пәрмендер

Kaspersky Security Center бағдарламасы ұялы құрылғыларды басқаруға арналған пәрмендерді қолдайды.

Пәрмендер ұялы құрылғыларды қашықтан басқару үшін қолданылады. Мысалы, пәрмен арқылы ұялы құрылғы жоғалған жағдайда, құрылғыдан корпоративтік деректерді жоюға болады.

Басқарылатын ұялы құрылғылардың келесі түрлері үшін пәрмендерді пайдалануға болады:

- iOS MDM құрылғылары
- Kaspersky Endpoint Security (KES) құрылғылары

Құрылғының әрбір түрі әртүрлі пәрмендер жиынтығын қолдайды.

Кейбір пәрмендердің ерекшеліктері

- Құрылғылардың барлық түрлері үшін **Зауыттық параметрлерге қалпына келтіру** пәрмені сәтті орындалған жағдайда, барлық деректер құрылғыдан жойылады, құрылғы конфигурациялары зауыттық конфигурацияларға дейін қалпына келтіріледі.
- iOS MDM құрылғылары үшін, **Корпоративтік деректерді жою** пәрмені сәтті орындалған жағдайда құрылғыдан барлық орнатылған конфигурациялық профильдер, provisioning профильдері, iOS MDM профилі және **iOS MDM профилімен бірге жою** қойылған қолданбалар жойылады.
- KES құрылғылары үшін, **Корпоративтік деректерді жою** пәрмені сәтті орындалған жағдайда, құрылғыдан корпоративтік деректер, Контактілердегі жазбалар, SMS тарихы, қоңыраулар журналы, күнтізбе, интернетке қосылу параметрлері, Google™ есептік жазбасынан басқа пайдаланушы есептік жазбалары жойылады. KES құрылғылары үшін жад картасынан қосымша деректер жойылады.
- **Орналасқан жерді анықтау** пәрменін KES құрылғыларына жібермес бұрын, сізге осы пәрменді ұйымыңызға немесе қызметкерлердің біріне тиесілі жоғалған құрылғыны рұқсатпен іздеу үшін қолданатыныңызды растау қажет болады. **Орналасқан жерді анықтау** пәрменін қабылдайтын ұялы құрылғы бұғатталмаған.

Ұялы құрылғыларға арналған пәрмендер тізімі

Төмендегі кестеде iOS MDM құрылғыларына арналған пәрмендер тізімі берілген.

Ұялы құрылғыларды басқаруға арналған қолдау көрсетілетін пәрмендер тізімі: iOS MDM құрылғылары

Пәрмендер	Пәрменді орындау нәтижесі
Құлыптау	Ұялы құрылғы бұғатталды.
Құлпын ашу	Ұялы құрылғыны PIN-кодпен бұғаттау өшірулі. Бұрын орнатылған PIN коды қалпына келтірілді.
Зауыттық параметрлерге қалпына келтіру	Ұялы құрылғыдан барлық деректер жойылды, ұялы құрылғы конфигурациялары зауыттық конфигурацияларға дейін қалпына келтірілді.
Корпоративтік деректерді жою	Барлық орнатылған конфигурациялық профильдер, provisioning профильдері, iOS MDM профилі және **iOS MDM профилімен бірге жою** жалаушасы қойылған қолданбалар жойылды.
Құрылғыны синхрондау	Ұялы құрылғы деректері Басқару серверімен синхрондалған.
Профильді орнату	Конфигурациялық профиль ұялы құрылғыға орнатылған.
Профильді жою	Конфигурациялық профиль ұялы құрылғыдан жойылды.
Provisioning профилін орнату	Provisioning профилі ұялы құрылғыға орнатылған.

Пәрмендер	Пәрменді орындау нәтижесі
Provisioning профилін жою	Provisioning профилі ұялы құрылғыдан жойылған.
Бағдарламаны орнату	Қолданба ұялы құрылғыға орнатылған.
Бағдарламаны жою	Қолданба ұялы құрылғыдан жойылды.
Өтеу кодын енгізу	Ақылы қолданбаның өтеу коды енгізілді.
Роуминг параметрлерін теңшеу	Деректер роумингі және дауыстық роуминг қосулы немесе өшірулі.

Төмендегі кестеде KES құрылғыларына арналған пәрмендер тізімі берілген.

Ұялы құрылғыларды басқаруға арналған қолдау көрсетілетін пәрмендер тізімі: iOS MDM құрылғылары

Пәрмен	Пәрменді орындау нәтижесі
Құлыптау	Ұялы құрылғы бұғатталды.
Құлпын ашу	Ұялы құрылғыны PIN-кодпен бұғаттау өшірулі. Бұрын орнатылған PIN коды қалпына келтірілді.
Зауыттық параметрлерге қалпына келтіру	Ұялы құрылғыдан барлық деректер жойылды, ұялы құрылғы конфигурациялары зауыттық конфигурацияларға дейін қалпына келтірілді.
Корпоративтік деректерді жою	Корпоративтік деректер, Контактілердегі жазбалар, SMS тарихы, қоңыраулар журналы, күнтізбе, интернетке қосылу параметрлері, Google есептік жазбасынан басқа пайдаланушы есептік жазбалары жойылды. Жад картасынан деректер жойылды.
Құрылғыны синхрондау	Ұялы құрылғы деректері Басқару серверімен синхрондалған.
Құрылғының орналасқан жерін анықтау	Ұялы құрылғының орналасқан жері Google Карталар™ қызметінде анықталған және көрсетілген. Ұялы байланыс операторы SMS және интернет беру үшін ақы алады.
Құжат фотосуреті	Ұялы құрылғы бұғатталды. Фотосурет құрылғының алдыңғы камерасымен жасалған және Басқару серверінде сақталған. Фотосуреттерді пәрмендер журналынан көруге болады. Ұялы байланыс операторы SMS және интернет беру үшін ақы алады.
Дабыл сигналы	Ұялы құрылғы дыбыстық сигнал шығарады.

Firebase Cloud Messaging қолдану

Kaspersky Security Center-де Android операциялық жүйесі басқаратын KES құрылғыларына пәрмендерді уақтылы жеткізу үшін push-нотификациялар механизмі пайдаланылады. KES құрылғылары мен Басқару сервері арасындағы push-нотификациялар Firebase Cloud Messaging (бұдан әрі – FCM) сервисінің көмегімен жүзеге асырылады. Kaspersky Security Center Басқару консолінде KES құрылғыларын осы сервиске қосу үшін Cloud Messaging сервисінің параметрлерін көрсете аласыз.

Firebase Cloud Messaging параметрлерін алу үшін Google есептік жазбаңыз болуы керек.

FCM қолдануды қосу үшін:

1. Басқару консолінен **Мобильді құрылғыларды басқару** түйіні мен **Ұялы құрылғылар** торабын таңдаңыз.
2. **Ұялы құрылғылар** қалтасының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.
3. Қалта сипаттары терезесінен **Firebase Cloud Messaging параметрлері** бөлімін таңдаңыз.
4. **Firebase жобасының нөмірі** өрісінде Sender ID FCM енгізіңіз.
5. **Жеке кілт файлы (JSON пішімінде)** өрісінде жеке кілт файлын таңдаңыз.

Басқару серверімен келесі жолы синхрондау кезінде, Android операциялық жүйесі басқаратын KES құрылғылары Firebase Cloud Messaging қызметіне қосылатын болады.

Firebase Cloud Messaging параметрлерін **Параметрлер бастапқы мәнге келтірілуде** түймесі арқылы өзгерте аласыз.

Пәрмендерді жіберу

Пәрменді пайдаланушының ұялы құрылғысына жіберу үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Пәрменді жіберу қажет болған пайдаланушы ұялы құрылғысын таңдаңыз.

3. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

4. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде ұялы құрылғыға жіберу қажет пәрменнің атауы бар бөлімге өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Таңдалған пәрменге байланысты, **Пәрмен жіберу** түймесін басқаннан кейін пәрменнің қосымша параметрлерін конфигурациялау терезесі ашылуы мүмкін. Мысалы, ұялы құрылғыдан provisioning профилін жоюға арналған жіберу кезінде бағдарлама ұялы құрылғыдан жою қажет provisioning профилін таңдауды ұсынады. Терезеде пәрменнің қосымша параметрлерін көрсетіп, таңдауыңызды растаңыз. Содан соң, пәрмен ұялы құрылғыға жіберіледі.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады.

   Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

   Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

Пәрмендер журналында пәрмендер күйлерін қарау

Қолданба мобильдік құрылғыларға жіберілген барлық пәрмен туралы ақпаратты пәрмендер журналына сақтайды. Пәрмендер журналында әрбір пәрменнің мобильдік құрылғыға жіберілген уақыты мен күні, олардың сәйкес күйлері және пәрменді орындау нәтижелерінің егжей-тегжейлі сипаттамалары туралы ақпарат бар. Мысалы, пәрменді орындау сәтсіз болған жағдайда, журнал қате себебін көрсетеді. Пәрмендер журналындағы жазбалар 30 күннен асырмай сақталады.

Ұялы құрылғыларға жіберілген пәрмендер келесі күйлерге ие болуы мүмкін:

- *Орындалуда* – пәрмен ұялы құрылғыға жіберілді.
- *Аяқталды* – пәрменнің орындалуы сәтті аяқталды.
- *Қатемен аяқталды* – пәрменді орындау мүмкін болмады.
- *Жойылуда* – пәрмен ұялы құрылғыға жіберілген пәрмендер кезегінен жойылуда.

- *Жойылды* – пәрмен ұялы құрылғыға жіберілген пәрмендер кезегінен сәтті түрде жойылды.
- *Жою қатемен аяқталды* – пәрменді ұялы құрылғыға жіберілген пәрмендер кезегінен жою мүмкін болмады.

Бағдарлама әрбір ұялы құрылғы үшін пәрмендер журналын жүргізеді.

Ұялы құрылғыға жіберілген пәрмендер журналын қарау үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Тізімнен пәрмендер журналын қарағыңыз келетін ұялы құрылғыны қараңыз.

3. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

   Ұялы құрылғыларды басқаруға арналған пәрмендер терезесі ашылады. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінің бөлімдері ұялы құрылғыға жіберуге болатын пәрмендерге сай келеді.

4. Өзіңізге қажетті пәрмендері бар бөлімдерді таңдап, пәрмендерді жіберу және орындау туралы ақпаратты **Пәрмендер журналы** блогында қараңыз.

Пәрмендер журналы блогында ұялы құрылғыға жіберілген пәрмендер тізімін және пәрмендер туралы ақпаратты қарай аласыз. **Пәрмендерді көрсету** сүзгісінің көмегімен тізімде таңдалған күйі бар пәрмендерді ғана қарауға болады.

Ұялы құрылғыларға арналған сертификаттармен жұмыс істеу

Бұл бөлімде ұялы құрылғылардың сертификаттарымен жұмыс істеу туралы ақпарат келтірілген.

Мобильді құрылғыларға арналған түбірлік сертификат жасалғаннан кейін 700 күн ішінде жарамды. Резервтік сертификат жарамдылық мерзімінің аяқталу күніне дейін 60 күн бұрын жасалады. Резервтік сертификат жасау уақытын келесі пәрмен арқылы өзгертуге болады:

```
klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v
<секундтарда күту уақыты>
```

Резервтік сертификат жасауға кететін уақыт барлық басқарылатын мобильді құрылғылардың Басқару серверімен синхрондауы және сертификат алуы үшін жеткілікті болуы керек.

klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Мобильді құрылғылар үшін түбірлік сертификатты қолмен жаңартуға қолдау көрсетілмейді.

Сертификаттарды орнату шеберін іске қосу

Сіз пайдаланушының ұялы құрылғысына келесі түрдегі сертификаттарды орната аласыз:

- ұялы құрылғыны сәйкестендіруге арналған жалпы сертификаттар;
- ұялы құрылғыда корпоративтік поштаны конфигурациялауға арналған пошталық сертификаттар;
- ұялы құрылғыда виртуалды жеке желіге қатынасуды конфигурациялау үшін VPN сертификаты.

Сертификатты пайдаланушының ұялы құрылғысына орнату үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Сертификаттар** салынған қалтасын таңдаңыз.
2. **Сертификаттар** қалтасының жұмыс аймағында **Сертификат қосу** сілтемесі бойынша сертификаттарды орнату шеберін іске қосыңыз.

Содан кейін, шебердің нұсқауларын орындаңыз.

Шебердің жұмысы барысында, сертификат жасалады, пайдаланушы сертификаттары тізіміне қосылады, бұдан бөлек, пайдаланушыға сертификатты ұялы құрылғыға жүктеу және орнату үшін сілтемесі бар хабарландыру жіберіледі. Барлық сертификаттар тізімін қарап шығуға және файлға экспорттауға болады. Сертификаттарды жоюға және қайта шығаруға, сондай-ақ олардың сипаттарын қарауға болады.

1-қадам. Сертификат түрін таңдау

Пайдаланушының ұялы құрылғысына орнату керек болған сертификат түрін көрсетіңіз:

- **Ұялы құрылғы сертификаты** – ұялы құрылғыны анықтау үшін.
- **Пошталық сертификат** – ұялы құрылғыда корпоративтік поштаны конфигурациялау үшін.
- **VPN сертификаты** – ұялы құрылғыда виртуалды жеке желіге қатынасуды конфигурациялау үшін.

2-қадам. Құрылғы түрін таңдау

Бұл терезе, бұған дейін **Пошталық сертификат** немесе **VPN сертификаты** сертификат түрі таңдалған болса ғана көрсетіледі.

Құрылғының операциялық жүйесінің түрін көрсетіңіз:

- **iOS MDM құрылғысы**. iOS MDM протоколы арқылы iOS MDM серверіне қосылатын ұялы құрылғыға сертификат орнату қажет болса, осы нұсқаны таңдаңыз.

- **Ұялы құрылғыларға арналған Kaspersky Security басқаруындағы KES-құрылғысы**. KES құрылғысына сертификат орнату қажет болса, осы нұсқаны таңдаңыз. Бұл жағдайда, сертификат пайдаланушыны анықтау үшін Басқару серверіне қосылған кезде пайдаланылады.

- **Пайдаланушы сертификатының негізінде түпнұсқалылықты тексерусіз Басқару серверіне қосылған KES құрылғысы**. Сертификат бойынша аутентификациясы жоқ KES құрылғысына сертификат орнату қажет болса, осы нұсқаны таңдаңыз. Бұл жағдайда, шебердің соңғы қадамында, **Пайдаланушыға хабарлау әдісі** терезесінде әкімші Басқару серверіне қосылу кезінде пайдаланушыны авторизациялау түрін таңдауы тиіс.

3-қадам. Пайдаланушыны таңдау

Сертификат орнатқыңыз келетін пайдаланушылар тізімінен, қауіпсіздік тобынан Active Directory таңдаңыз.

Пайдаланушыны таңдау терезесінде Kaspersky Security Center ішкі пайдаланушыларын іздей аласыз. Ішкі пайдаланушыны қосу үшін **Қосылуда** түймесін баса аласыз.

4-қадам. Сертификат көзін таңдау

Терезеде, Басқару сервері ұялы құрылғыны анықтайтын сертификат көзін таңдауға болады. Сертификатты келесі тәсілдердің бірімен белгілеуге болады:

- Басқару сервері арқылы автоматты түрде сертификат жасау және сертификатты құрылғыға жеткізу.

- Бұған дейін жасалған сертификат файлын көрсетіңіз. Алдыңғы қадамда бірнеше пайдаланушы таңдалған болса, бұл тәсіл қолжетімді болмайды.

Пайдаланушыға оның ұялы құрылғысына арналған сертификат жасау туралы хабарландыру жіберу керек болса, **Сертификатты жариялау** жалаушасын қойыңыз.

Егер пайдаланушының ұялы құрылғысы бұған дейін сертификат бойынша авторизацияланған болса және жаңа сертификат алу үшін есептік жазбаның атауы мен құпиясөзін көрсетудің қажеті болмаса, **Сертификатты жариялау** жалаушасын алып тастаңыз. Бұл жағдайда, **Пайдаланушыға хабарлау әдісі** терезесі көрсетілмейді.

5-қадам. Сертификаттарға тег белгілеу

Құрылғы түрі iOS MDM құрылғысы таңдалған болса, **Сертификат тегі** терезесі көрсетіледі.

Ашылмалы тізімнен, пайдаланушының iOS MDM құрылғысы сертификаты үшін тег белгілей аласыз. Тағайындалған тег сертификатында Kaspersky Device Management for iOS саясатының сипаттарында осы тег үшін белгіленген арнайы параметрлер болуы мүмкін.

Ашылмалы тізім *Сертификат үлгісі 1*, *Сертификат үлгісі 2* немесе *Сертификат үлгісі 3* тегін таңдауды сұрайды. Тегтерді келесі бөлімдерде конфигурациялауға болады:

- **Пошталық сертификат Сертификат түрі** терезесінде таңдалған болса, оған арналған тегтерді мобильдік құрылғыларға арналған Exchange ActiveSync есептік жазбасының сипаттарында конфигурациялауға болады (**Басқарылатын құрылғылар** → **Саясаттар** → iOS саясат сипаттарына арналған Kaspersky құрылғысын басқару > **Exchange ActiveSync** бөлімі → **Қосу** → **Кеңейтілген**).

- **Сертификат түрі** терезесінде **VPN сертификаты** таңдалған болса, оған арналған тегтерді мобильдік құрылғыларға арналған VPN сипаттарында конфигурациялауға болады (**Басқарылатын құрылғылар** → **Саясаттар** → iOS саясат сипаттарына арналған Kaspersky құрылғысын басқару → **VPN** бөлімі → **Қосу** → **Кеңейтілген**). VPN желісі үшін L2TP, PPTP немесе IPSec (Cisco™) қосылым түрі таңдалған болса, VPN сертификаттары үшін пайдаланылатын тегтерді конфигурациялау қолжетімді емес.

6-қадам. Сертификатты жариялау параметрлерінің сипаттамасы

Бұл терезеде сертификатты жариялаудың келесі параметрлерін көрсетуге болады:

- **Пайдаланушыға жаңа сертификат туралы хабарламау**

  Пайдаланушыға ұялы құрылғысына сертификат жасау туралы хабарландыру жібергіңіз келмесе, осы параметрді қосыңыз. Бұл жағдайда, **Пайдаланушыға хабарлау әдісі** терезесі көрсетілмейді.

  > Бұл параметр тек Kaspersky Endpoint Security for Android қолданбасы орнатылған құрылғыларға қолданылады.

  Сіз бұл параметрді қосқыңыз келуі мүмкін, мысалы, егер пайдаланушының ұялы құрылғысы сертификаттың көмегімен анықталған болса, сондықтан жаңа сертификат алу үшін есептік жазбаның атауы мен құпиясөзін көрсетудің қажеті жоқ.

- **Құрылғыға бір сертификатты бірнеше рет алуға рұқсат беру (тек Kaspersky Endpoint Security for Android орнатылған құрылғылар үшін)**

  \Kaspersky Security Center бағдарламасы жақын арада жарамдылық мерзімі аяқталған немесе мақсатты құрылғыда табылмаған сайын сертификатты автоматты түрде қайта жіберуі үшін, осы параметрі қосыңыз.

  Сертификат, сертификаттың жарамдылық мерзімі біткенге дейін бірнеше күн қалғанда автоматты түрде қайта жіберіледі. Сіз Сертификаттарды шығару ережелері терезесінде күндер санын белгілей аласыз.

  Кейбір жағдайларда сертификаттарды құрылғылардан табу мүмкін емес. Мысалы, бұл жағдай, егер пайдаланушы Kaspersky қауіпсіздік қолданбасын құрылғыға қайта орнатса немесе құрылғыны зауыттық параметрлерге қалпына келтірсе орын алуы мүмкін. Бұл жағдайда, Kaspersky Security Center бағдарламасы, құрылғы келесі рет Басқару серверіне қосылуға әрекеттенгенде құрылғы идентификаторын тексереді. Егер құрылғыда сертификатты беру кезіндегідей идентификатор болса, бағдарлама сертификатты құрылғыға береді.

7-қадам. Пайдаланушыға хабарлау әдісін таңдау

> Құрылғы түрі ретінде **iOS MDM құрылғысы** нұсқасы таңдалса немесе **Пайдаланушыға жаңа сертификат туралы хабарламау** нұсқасы таңдалса, бұл терезе көрсетілмейді.

Пайдаланушыға хабарлау әдісі терезесінде пайдаланушыға сертификатты ұялы құрылғыға орнату туралы хабарлау параметрлерін конфигурациялауға болады.

Аутентификация әдісі өрісінде пайдаланушы түпнұсқалық растамасы түрін көрсетіңіз:

- **Тіркелгі деректері (домен немесе бүркеншік аты)**

  Бұл жағдайда, пайдаланушы жаңа сертификат алу үшін Kaspersky Security Center ішкі пайдаланушысының құпиясөзін немесе домендік құпиясөзін пайдаланады.

- **Бір реттік құпиясөз**

  Бұл жағдайда, пайдаланушы электрондық поштаға немесе SMS арқылы жіберілетін бір реттік құпиясөзді алады. Бұл құпиясөз жаңа сертификат алу үшін көрсетілуі керек.

  Егер сіз **Сертификатты жариялау параметрлері** терезесінде **Құрылғыға бір сертификатты бірнеше рет алуға рұқсат беру (тек Kaspersky қауіпсіздік қосымшалары орнатылған құрылғылар үшін)** параметрін қоссаңыз, бұл параметр **Құпиясөз** болып өзгереді.

- **Құпиясөз**

  Бұл жағдайда, құпиясөз, сертификат пайдаланушыға жіберілген сайын қолданылады.

  Егер сіз **Сертификатты жариялау параметрлері** терезесінде **Құрылғыға бір сертификатты бірнеше рет алуға рұқсат беру (тек Kaspersky қауіпсіздік қосымшалары орнатылған құрылғылар үшін)** параметрін қоссаңыз, бұл параметр **Бір реттік құпиясөз** болып өзгереді.

Бұл өріс **Сертификат түрі** терезесінде **Ұялы құрылғы сертификаты** таңдаған болсаңыз немесе құрылғы түрі ретінде **Пайдаланушы сертификатының негізінде түпнұсқалылықты тексерусіз Басқару серверіне қосылған KES құрылғысы** таңдаған болсаңыз көрсетіледі.

Пайдаланушыны хабарландыру нұсқасын таңдаңыз:

- **Шебердің жұмысы аяқталғаннан кейін аутентификациялау құпиясөзін көрсету**

  Осы параметрді таңдасаңыз, онда пайдаланушы атауы, пайдаланушының SAM есептік жазбасының атауы (Security Account Manager) және таңдалған пайдаланушылардың әрқайсысы үшін сертификат алуға арналған құпиясөз сертификаттарды орнату шеберінің соңғы қадамында көрсетілетін болады. Пайдаланушыны орнатылған сертификат туралы хабарландыру параметрлерін конфигурациялау қолжетімді емес болады.

  Бірнеше пайдаланушыға арналған сертификаттарды қосып жатсаңыз, сіз ұсынылған есептік деректерді файлға сақтай аласыз, бұл үшін сертификаттарды орнату шеберінің соңғы қадамында **Экспорт** түймесін басыңыз.

  > Сертификаттарды орнату шеберінің **Пайдаланушыға хабарлау әдісі** қадамында **Тіркелгі деректері (домен немесе бүркеншік аты)** тармағын таңдаған болсаңыз, бұл параметр қолжетімді болмайды.

- **Пайдаланушыға жаңа сертификат туралы хабарлау**

  Осы нұсқаны таңдау кезінде, сіз пайдаланушыны жаңа сертификат туралы хабарландыру параметрлерін конфигурациялай аласыз.

  - **Электрондық пошта арқылы**

    Электрондық пошта бойынша параметрлері блогында пайдаланушыға сертификатты өз ұялы құрылғысына орнату туралы электрондық пошта хабарлары көмегімен хабарлау параметрлерін конфигурациялай аласыз. Осылай хабарлау әдісі, SMTP сервері конфигурацияланған болса ғана қолжетімді.

    Хабарды қарап шығу және қажет болса, өзгерту үшін **Хабарды өңдеу** сілтемесінен өтіңіз.

  - **SMS арқылы**

    Осы параметрлер блогында пайдаланушыға сертификатты өз ұялы құрылғысына орнату туралы SMS хабарлары көмегімен хабарлау параметрлерін конфигурациялай аласыз. Осылай хабарлау әдісі, SMS хабарландырулары конфигурацияланған болса ғана қолжетімді.

    Хабарды қарап шығу және қажет болса, өзгерту үшін **Хабарды өңдеу** сілтемесінен өтіңіз.

8-қадам. Сертификат жасау

Бұл қадамда сертификат жасалады.

Шеберден шығу үшін **Аяқтау** түймесін баса аласыз.

Жасалған сертификат **Сертификаттар** қалтасының жұмыс аймағындағы сертификаттар тізімінде көрсетіледі.

Сертификаттарды шығару ережелерін конфигурациялау

Сертификаттар Басқару серверінде құрылғылардың түпнұсқалық растамасын жасау үшін қолданылады. Барлық басқарылатын ұялы құрылғылардың сертификаттары болуы тиіс. Сертификаттарды шығару тәсілін конфигурациялауға болады.

Сертификаттарды шығару ережелерін конфигурациялау үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Сертификаттар** салынған қалтасын таңдаңыз.

2. **Сертификаттар** қалтасының жұмыс аймағында, **Сертификат беру ережелерін конфигурациялау** түймесі арқылы **Сертификаттарды шығару ережелері** терезесін ашыңыз.

3. Сертификат түрінің атауы бар бөлімге өтіңіз:

   Ұялы құрылғы сертификаттарын шығару – мобильдік құрылғыларға арналған сертификаттар шығаруды конфигурациялау үшін.

   Пошталық сертификаттарды шығару – пошталық сертификаттарды шығаруды конфигурациялау үшін.

   VPN сертификаттарын шығару – VPN сертификаттарын шығаруды конфигурациялау үшін.

4. **Шығару параметрлері** блогында сертификатты шығаруды конфигурациялаңыз:

   - Сертификаттың күндердегі жарамдылық мерзімін көрсетіңіз.

     Мобильді құрылғыларға арналған сертификаттар түбірлік сертификаттың жарамдылық мерзімімен шектеледі. Түбірлік сертификаттың әрекет ету мерзімінен ұзағырақ сертификаттың жарамдылық мерзімін көрсетсеңіз, сертификаттың әрекет ету мерзімі жасалған кезде автоматты түрде өзгертіледі.

   - Сертификаттардың көзін таңдаңыз (**Басқару сервері** немесе **Сертификаттар қолмен белгіленеді**).

     Әдепкі бойынша, сертификаттардың көзі болып Басқару сервері таңдалған.

   - Сертификаттар үлгісін белгілеңіз (**Әдепкі үлгі**, **Басқа үлгі**).

     Үлгілер конфигурациясы, **PKI жүйесімен интеграциялау** бөлімінде жалпыға ортақ кілттер инфрақұрылымымен біріктіру мүмкіндігі конфигурацияланған болса, қолжетімді болады.

5. **Автоматты жаңартулар параметрлері** блогында сертификатты автоматты түрде жаңартуды конфигурациялаңыз:

   - **Сертификат (күннен) кейін аяқталған кезде келесіні жаңартыңыз** блогында мерзімі біткенге дейін қалған қанша күн ішінде сертификатты жаңарту керектігін көрсетіңіз.

   - Сертификаттарды автоматты түрде жаңартуды қосу үшін **Мүмкін болса, сертификатты автоматты түрде қайта шығару** жалаушасын қойыңыз.

6. **Құпиясөзбен қорғау** блогында сертификаттарды шифрсыздау кезінде құпиясөзді қолдануды қосыңыз және конфигурациялаңыз.

   Құпиясөзбен қорғау тек ұялы құрылғылар үшін ғана қолжетімді.

   a. **Сертификатты орнату кезінде құпиясөзді сұрау** жалаушасын қойыңыз.

   b. Сырғақтың көмегімен, шифрлауға арналған құпиясөзде таңбалардың ең көп санын конфигурациялаңыз.

7. **ОК** түймесін басыңыз.

Жалпыға ортақ кілттер инфрақұрылымымен біріктіру

Бағдарламаны жалпыға ортақ кілттер инфрақұрылымымен (Public Key Infrastructure, PKI) біріктіру, пайдаланушылардың домендік сертификаттарын шығаруды жеңілдету үшін қажет. Біріктіру нәтижесінде, сертификаттарды шығару автоматты түрде жүзеге асырылады.

PKI серверінің ең аз қолдау көрсетілетін нұсқасы – Windows Server 2008.

PKI жүйесімен интеграциялау үшін есептік жазбаны конфигурациялау керек. Есептік жазба келесі талаптарға сай келуі тиіс:

- Басқару сервері орнатылған құрылғының домендік пайдаланушысы мен әкімшісі болу;
- Басқару сервері орнатылған құрылғыда SeServiceLogonRight артықшылығына ие болу.

Тұрақты пайдаланушы профилін жасау үшін орнатылған Басқару сервері бар құрылғыға конфигурацияланған есептік жазбамен кемінде бір рет кіру керек. Осы пайдаланушының сертификаттар қоймасында, Басқару сервері бар құрылғыда доменнің әкімшілері ұсынған тіркеу агенті сертификатын орнату керек.

Жалпыға ортақ кілттер инфрақұрылымымен біріктіруді конфигурациялау үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Сертификаттар** салынған қалтасын таңдаңыз.

2. Жұмыс аймағында, **Сертификаттарды шығару ережелері** терезесінің **PKI жүйесімен интеграциялау** бөлімін ашу үшін **Ашық кілттердің инфрақұрылымымен интеграциялау** түймесін басыңыз.

   Сертификаттарды шығару ережелері терезесінің **PKI жүйесімен интеграциялау** бөлімі ашылады.

3. **Сертификаттар жазып беру мен PKI интеграциялау** жалаушасын қойыңыз.

4. **Есептік жазба** өрісінде, жалпыға ортақ кілттер инфрақұрылымымен біріктіру үшін қолданылатын пайдаланушының есептік жазбасының атауын көрсетіңіз.

5. **Құпиясөз** өрісінде есептік жазбаның домендік құпиясөзін көрсетіңіз.

6. **PKI жүйесіндегі сертификат үлгісінің атауы** тізімінде доменнің пайдаланушыларына сертификаттарды шығару үшін қолданылатын сертификаттың үлгісін таңдаңыз.

   Kaspersky Security Center бағдарламасында көрсетілген есептік жазбамен мамандандырылған қызмет іске қосылады. Бұл қызмет пайдаланушылардың домендік сертификаттарын шығару үшін жауап береді. Қызмет, **Тізімді жаңарту** түймесі бойынша сертификаттардың үлгілері тізімі жүктелген кезде немесе сертификатты шығару кезінде іске қосылады.

7. Параметрлерді сақтау үшін **OK** түймесін басыңыз.

Біріктіру нәтижесінде, сертификаттарды шығару автоматты түрде жүзеге асырылады.

Kerberos Constrained Delegation қолдауын қосу

Бағдарлама Kerberos Constrained Delegation қолдануды қолдамайды.

Kerberos Constrained Delegation қолдауын қосу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын ашыңыз.

2. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.

3. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.

4. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

5. iOS MDM сервері сипаттары терезесінде **Параметрлер** бөлімін таңдаңыз.

6. **Параметрлер** бөлімінде **Kerberos Constrained Delegation әдісімен үйлесімділікті қамтамасыз ету** жалаушасын қойыңыз.

7. **OK** түймесін басыңыз.

iOS ұялы құрылғыларын басқарылатын құрылғылар тізіміне қосу

iOS ұялы құрылғысын басқарылатын құрылғылар тізіміне қосу үшін, құрылғыға жалпы сертификатты жеткізіп, орнату керек. Жалпы сертификаттар Басқару серверінің ұялы құрылғыларды идентификациялауы үшін қолданылады. iOS ұялы құрылғысына арналған жалпы сертификат iOS MDM профилі құрамында жеткізіледі. Жалпы сертификатты жеткізіп, ұялы құрылғыға орнатқаннан кейін, ұялы құрылғы басқарылатын құрылғылар тізімінде көрсетіледі.

Kaspersky бұдан былай Kaspersky Safe Browser-ді қолдамайды.

Сіз ұялы құрылғыны қосу шеберінің көмегімен пайдаланушылардың ұялы құрылғыларын басқарылатын құрылғылар тізіміне қоса аласыз.

iOS құрылғысын жалпы сертификаттың көмегімен Басқару серверіне қосу үшін:

1. Ұялы құрылғыны қосу шеберін келесі тәсілдердің бірімен іске қосыңыз:

   - **Пайдаланушылардың есептік жазбалары** қалтасының мәнмәтіндік мәзірінде:

     1. **Кеңейтілген** қалтасындағы консоль шежіресінен **Пайдаланушылардың есептік жазбалары** салынған қалтасын таңдаңыз.

     2. **Пайдаланушылардың есептік жазбалары** қалтасының жұмыс аймағында мобильдік құрылғыларды басқарылатын құрылғылар тізіміне қосқыңыз келетін пайдаланушыларды, қауіпсіздік топтарын немесе пайдаланушылардың Active Directory қауіпсіздік тобын таңдаңыз.

     3. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Ұялы құрылғыны қосу** тармағын таңдаңыз.

        Жаңа ұялы құрылғыны қосу шебері іске қосылды.

   - **Ұялы құрылғылар** қалтасының жұмыс аймағында **Ұялы құрылғыны қосу** түймесін басыңыз:

     1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

     2. **Ұялы құрылғылар** салынған қалтасының жұмыс аймағында **Ұялы құрылғыны қосу** түймесін басыңыз.

        Жаңа ұялы құрылғыны қосу шебері іске қосылды.

2. **Операциялық жүйе** шебері терезесінде **iOS** ұялы құрылғысының операциялық жүйесінің түрін таңдаңыз.

3. **iOS MDM серверін таңдау** бетінде iOS MDM серверін таңдаңыз.

4. **Ұялы құрылғыларын басқарғыңыз келетін пайдаланушыларды таңдаңыз** қалтасының жұмыс аймағында мобильдік құрылғыларды басқарылатын құрылғылар тізіміне қосқыңыз келетін пайдаланушыларды, қауіпсіздік топтарын немесе пайдаланушылардың Active Directory қауіпсіздік тобын таңдаңыз.

   Пайдаланушылардың есептік жазбалары қалтасының мәнмәтіндік мәзірінде **Ұялы құрылғыны қосу** тармағын таңдап шеберді іске қосқан болсаңыз, бұл қадамды өткізіп жібересіз.

Пайдаланушы есептік жазбасын тізімге қосқыңыз келсе, **Қосылуда** түймесін басыңыз, содан соң ашылған терезеде пайдаланушы есептік жазбасының параметрлерін көрсетіңіз. Пайдаланушы есептік жазбасының сипаттарын өзгерткіңіз немесе қарағыңыз келсе, тізімдегі пайдаланушы есептік жазбасын таңдап, **Сипаттар** түймесін басыңыз.

5. **Сертификат көзі** шебер бетінде Басқару серверінің ұялы құрылғыны идентификациялауына мүмкіндік беретін жалпы сертификатты жасау тәсілін көрсетіңіз. Сіз жалпы сертификатты келесі екі тәсілдің бірімен белгілей аласыз:

   - **Басқару серверінің құралдары арқылы сертификат жазып беру**

     Сертификатты әлі жасамаған болсаңыз, оны Басқару сервері аспаптарының көмегімен жасау үшін осы параметрді таңдаңыз.

     Осы нұсқа таңдалған болса, онда iOS MDM профиліне Басқару сервері жасаған сертификатпен автоматты түрде қол қойылады.

     Әдепкі бойынша, осы нұсқа таңдалады.

   - **Сертификат файлын көрсету**

     Бұған дейін жасалған сертификат файлын көрсету үшін осы параметрді таңдаңыз.

     Алдыңғы қадамда бірнеше пайдаланушы таңдалған болса, бұл тәсіл қолжетімді болмайды.

6. **Пайдаланушыға хабарлау әдісі** шебер бетінде ұялы құрылғы пайдаланушысын сертификаттың жасалғаны туралы SMS-хабарлама немесе электрондық пошта арқылы хабарландыру параметрлерін конфигурациялаңыз:

   - **QR кодын шеберден көрсету**

     Осы нұсқаны таңдаған кезде, орнату пакетіне сілтеме, құрылғыны қосу шебері жұмысының соңғы қадамында көрсетіледі.

     > Құрылғыны қосу үшін бірнеше пайдаланушы таңдалған болса, бұл нұсқа қолжетімді болмайды.

   - **QR кодын пайдаланушыға жіберу**

     Осы нұсқаны таңдаған кезде, пайдаланушыны жаңа ұялы құрылғының қосылғаны туралы хабарландыру параметрлерін конфигурациялауыңызға болады.

     Электрондық пошта мекенжайы түрін таңдауға, қосымша мекенжайды көрсетуге және хабарлама мәтінін түзетуге болады. SMS хабарларын жіберу үшін пайдаланушы телефонының түрін таңдауға, қосымша телефон нөмірін көрсетуге және жіберілетін SMS хабары мәтінін түзетуге де болады.

     SMTP сервері конфигурацияланбаған болса, пайдаланушыларға электрондық пошта хабарламаларын жіберу мүмкін болмайды. SMS хабарландыруы қосылмаған болса, пайдаланушыларға SMS хабарларын жіберу мүмкін емес.

7. Шебердің жұмысын аяқтау үшін **Нәтиже** шебер бетінде **Дайын** түймесін басыңыз.

Нәтижесінде, iOS MDM профилі Kaspersky Security Center Веб-серверінде автоматты түрде жарияланады. Ұялы құрылғының пайдаланушысы Веб-серверден iOS MDM профилін жүктеуге арналған сілтемесі бар хабарландыру алады. Пайдаланушы алынған сілтемеден өз бетінше өтеді. Содан соң, ұялы құрылғының операциялық жүйесі пайдаланушыдан iOS MDM профилін орнатуға келісім сұрайды. iOS MDM профилі ұялы құрылғыға жүктелуі үшін, пайдаланушы iOS MDM профилін орнатуға келісім беруі тиіс. iOS MDM профилін жүктеп, Басқару серверімен синхрондалғаннан кейін, үшін ұялы құрылғы консоль шежіресінің **Мобильді құрылғыларды басқару** қалтасына салынған **Ұялы құрылғылар** қалтасында көрсетіледі.

Пайдаланушы Kaspersky Security Center Веб-серверінде алынған сілтеме арқылы өтуі үшін, оның ұялы құрылғысынан 8061-порт бойынша Басқару серверіне қосылу қолжетімді болуы қажет.

Android ұялы құрылғыларын басқарылатын құрылғылар тізіміне қосу

Android ұялы құрылғысын басқарылатын құрылғылар тізіміне қосу үшін, құрылғыға Kaspersky Endpoint Security for Android қолданбасын жеткізіп, жалпы сертификатты орнату керек. Жалпы сертификаттар Басқару серверінің ұялы құрылғыларды идентификациялауы үшін қолданылады. Жалпы сертификатты жеткізіп, ұялы құрылғыға орнатқаннан кейін, ұялы құрылғы басқарылатын құрылғылар тізімінде көрсетіледі.

Сіз ұялы құрылғыны қосу шеберінің көмегімен пайдаланушылардың ұялы құрылғыларын басқарылатын құрылғылар тізіміне қоса аласыз. Жаңа ұялы құрылғыны қосу шебері жалпы сертификат пен Kaspersky Endpoint Security for Android қолданбасын жеткізудің және орнатудың екі тәсілін ұсынады:

- Google Play дүкеніне сілтеме арқылы.
- Kaspersky Security Center веб-серверіне сілтеме арқылы.

  Орнату үшін Басқару серверінде тарату үшін сақталған Kaspersky Endpoint Security for Android орнату пакеті қолданылады.

Жаңа ұялы құрылғыны қосу шеберін іске қосу

Ұялы құрылғыны қосу шеберін келесі тәсілдердің бірімен іске қосыңыз:

- **Пайдаланушылардың есептік жазбалары** қалтасының мәнмәтіндік мәзірінде:

  1. **Кеңейтілген** қалтасындағы консоль шежіресінен **Пайдаланушылардың есептік жазбалары** салынған қалтасын таңдаңыз.
  2. **Пайдаланушылардың есептік жазбалары** қалтасының жұмыс аймағында мобильдік құрылғыларды басқарылатын құрылғылар тізіміне қосқыңыз келетін пайдаланушыларды, қауіпсіздік топтарын немесе пайдаланушылардың Active Directory қауіпсіздік тобын таңдаңыз.
  3. Пайдаланушы есептік жазбасының мәнмәтіндік мәзірінде **Ұялы құрылғыны қосу** тармағын таңдаңыз.

     Жаңа ұялы құрылғыны қосу шебері іске қосылды.

- **Ұялы құрылғылар** қалтасының жұмыс аймағында **Ұялы құрылғыны қосу** түймесін басыңыз:

  1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.
  2. **Ұялы құрылғылар** салынған қалтасының жұмыс аймағында **Ұялы құрылғыны қосу** түймесін басыңыз.

     Жаңа ұялы құрылғыны қосу шебері іске қосылды.

Android ұялы құрылғысын Google Play сілтемесі арқылы қосу

Google Play сілтемесін пайдаланып, Kaspersky Endpoint Security for Android қолданбасын және ұялы құрылғыға арналған жалпы сертификатты орнату үшін:

1. Жаңа ұялы құрылғыны қосу шебері іске қосылды.

2. **Операциялық жүйе** шебері терезесінде **Android** ұялы құрылғысының операциялық жүйесінің түрін таңдаңыз.

3. Шебердің **Құрылғыларға Kaspersky Endpoint Security for Android орнату әдісі** бетінде **Бағдарламаны Google Play-ден жүктеп алу** тармағын таңдаңыз.

4. Шебердің **Ұялы құрылғыларын басқарғыңыз келетін пайдаланушыларды таңдаңыз** бетінде мобильдік құрылғыларды басқарылатын құрылғылар тізіміне қосқыңыз келетін пайдаланушыларды, қауіпсіздік топтарын немесе пайдаланушылардың Active Directory қауіпсіздік топтарын таңдаңыз.

   Шебер **Пайдаланушылардың есептік жазбалары** қалтасының контекстік мәзіріндегі **Ұялы құрылғыны қосу** опциясын таңдау арқылы іске қосылса, бұл қадам өткізіп жіберіледі.

   Пайдаланушы есептік жазбасын тізімге қосқыңыз келсе, **Қосылуда** түймесін басыңыз, содан соң ашылған терезеде пайдаланушы есептік жазбасының параметрлерін көрсетіңіз. Пайдаланушы есептік жазбасының сипаттарын өзгерткіңіз немесе қарағыңыз келсе, тізімдегі пайдаланушы есептік жазбасын таңдап, **Сипаттар** түймесін басыңыз.

5. **Сертификат көзі** шебер бетінде Басқару серверінің ұялы құрылғыны идентификациялауына мүмкіндік беретін жалпы сертификатты жасау тәсілін көрсетіңіз. Сіз жалпы сертификатты келесі екі тәсілдің бірімен белгілей аласыз:

   - **Басқару серверінің құралдары арқылы сертификат жазып беру**

     Сертификатты әлі жасамаған болсаңыз, оны Басқару сервері аспаптарының көмегімен жасау үшін осы параметрді таңдаңыз.

     Егер бұл параметр таңдалса, сертификат автоматты түрде Басқару сервері арқылы жазылады.

     Әдепкі бойынша, осы нұсқа таңдалады.

   - **Сертификат файлын көрсету**

     Бұған дейін жасалған сертификат файлын көрсету үшін осы параметрді таңдаңыз.

     Алдыңғы қадамда бірнеше пайдаланушы таңдалған болса, бұл тәсіл қолжетімді болмайды.

6. **Пайдаланушыға хабарлау әдісі** шебер бетінде ұялы құрылғы пайдаланушысын сертификаттың жасалғаны туралы SMS-хабарлама немесе электрондық пошта арқылы хабарландыру параметрлерін конфигурациялаңыз:

   - **QR кодын шеберден көрсету**

     Осы нұсқаны таңдаған кезде, орнату пакетіне сілтеме, құрылғыны қосу шебері жұмысының соңғы қадамында көрсетіледі.

     Құрылғыны қосу үшін бірнеше пайдаланушы таңдалған болса, бұл нұсқа қолжетімді болмайды.

- **QR кодын пайдаланушыға жіберу**

  Осы нұсқаны таңдаған кезде, пайдаланушыны жаңа ұялы құрылғының қосылғаны туралы хабарландыру параметрлерін конфигурациялауыңызға болады.

  Электрондық пошта мекенжайы түрін таңдауға, қосымша мекенжайды көрсетуге және хабарлама мәтінін түзетуге болады. SMS хабарларын жіберу үшін пайдаланушы телефонының түрін таңдауға, қосымша телефон нөмірін көрсетуге және жіберілетін SMS хабары мәтінін түзетуге де болады.

  SMTP сервері конфигурацияланбаған болса, пайдаланушыларға электрондық пошта хабарламаларын жіберу мүмкін болмайды. SMS хабарландыруы қосылмаған болса, пайдаланушыларға SMS хабарларын жіберу мүмкін емес.

7. Шебердің жұмысын аяқтау үшін **Нәтиже** шебер бетінде **Дайын** түймесін басыңыз.

Kaspersky Endpoint Security for Android шебердің жұмысы нәтижесінде, пайдаланушының ұялы құрылғысына жүктеп алу үшін сілтеме және QR коды жіберілетін болады. Пайдаланушы сілтемені басады немесе QR кодын сканерлейді. Содан кейін мобильдік құрылғының операциялық жүйесі пайдаланушыдан Kaspersky Endpoint Security for Android орнатылымын қабылдауды сұрайды. Kaspersky Endpoint Security for Android қолданбасын жүктеп алып, орнатқаннан кейін, ұялы құрылғы Басқару серверіне қосылып, жалпы сертификатты жүктеп алады. Сертификатты ұялы құрылғыға орнатқаннан кейін, бұл құрылғы консоль шежіресінің **Мобильді құрылғыларды басқару** қалтасына салынған **Ұялы құрылғылар** қалтасында көрсетілетін болады.

Kaspersky Security Center Web веб-серверіне сілтеме арқылы Android ұялы құрылғысын қосу

Орнату үшін Басқару серверінде жарияланған Kaspersky Endpoint Security for Android орнату пакеті қолданылады.

Веб-серверге сілтемені пайдаланып, Kaspersky Endpoint Security for Android қолданбасын және ұялы құрылғыға арналған жалпы сертификатты орнату үшін:

1. Жаңа ұялы құрылғыны қосу шебері іске қосылды.

2. **Операциялық жүйе** шебері терезесінде **Android** ұялы құрылғысының операциялық жүйесінің түрін таңдаңыз.

3. Шебердің **Құрылғыларға Kaspersky Endpoint Security for Android орнату әдісі** бетінде **Бағдарламаны орнату пакетін Kaspersky Security Center-ден жүктеп алу** тармағын таңдаңыз.

   Төмендегі өрісте орнату пакетін таңдаңыз немесе **Жаңа** түймесі арқылы жаңа орнату пакетін жасаңыз.

4. Шебердің **Ұялы құрылғыларын басқарғыңыз келетін пайдаланушыларды таңдаңыз** бетінде мобильдік құрылғыларды басқарылатын құрылғылар тізіміне қосқыңыз келетін пайдаланушыларды, қауіпсіздік топтарын немесе пайдаланушылардың Active Directory қауіпсіздік топтарын таңдаңыз.

   Шебер **Пайдаланушылардың есептік жазбалары** қалтасының контекстік мәзіріндегі **Ұялы құрылғыны қосу** опциясын таңдау арқылы іске қосылса, бұл қадам өткізіп жіберіледі.

   Пайдаланушы есептік жазбасын тізімге қосқыңыз келсе, **Қосылуда** түймесін басыңыз, содан соң ашылған терезеде пайдаланушы есептік жазбасының параметрлерін көрсетіңіз. Пайдаланушы есептік жазбасының сипаттарын өзгерткіңіз немесе қарағыңыз келсе, тізімдегі пайдаланушы есептік жазбасын таңдап, **Сипаттар** түймесін басыңыз.

5. **Сертификат көзі** шебер бетінде Басқару серверінің ұялы құрылғыны идентификациялауына мүмкіндік беретін жалпы сертификатты жасау тәсілін көрсетіңіз. Сіз жалпы сертификатты келесі екі тәсілдің бірімен белгілей аласыз:

   - **Басқару серверінің құралдары арқылы сертификат жазып беру**

     Сертификатты әлі жасамаған болсаңыз, оны Басқару сервері аспаптарының көмегімен жасау үшін осы параметрді таңдаңыз.

     Егер бұл параметр таңдалса, сертификат автоматты түрде Басқару сервері арқылы жазылады.

     Әдепкі бойынша, осы нұсқа таңдалады.

   - **Сертификат файлын көрсету**

     Бұған дейін жасалған сертификат файлын көрсету үшін осы параметрді таңдаңыз.

     Алдыңғы қадамда бірнеше пайдаланушы таңдалған болса, бұл тәсіл қолжетімді болмайды.

6. **Пайдаланушыға хабарлау әдісі** шебер бетінде ұялы құрылғы пайдаланушысын сертификаттың жасалғаны туралы SMS-хабарлама немесе электрондық пошта арқылы хабарландыру параметрлерін конфигурациялаңыз:

   - **QR кодын шеберден көрсету**

     Осы нұсқаны таңдаған кезде, орнату пакетіне сілтеме, құрылғыны қосу шебері жұмысының соңғы қадамында көрсетіледі.

     > Құрылғыны қосу үшін бірнеше пайдаланушы таңдалған болса, бұл нұсқа қолжетімді болмайды.

   - **QR кодын пайдаланушыға жіберу**

     Осы нұсқаны таңдаған кезде, пайдаланушыны жаңа ұялы құрылғының қосылғаны туралы хабарландыру параметрлерін конфигурациялауыңызға болады.

     Электрондық пошта мекенжайы түрін таңдауға, қосымша мекенжайды көрсетуге және хабарлама мәтінін түзетуге болады. SMS хабарларын жіберу үшін пайдаланушы телефонының түрін таңдауға, қосымша телефон нөмірін көрсетуге және жіберілетін SMS хабары мәтінін түзетуге де болады.

     SMTP сервері конфигурацияланбаған болса, пайдаланушыларға электрондық пошта хабарламаларын жіберу мүмкін болмайды. SMS хабарландыруы қосылмаған болса, пайдаланушыларға SMS хабарларын жіберу мүмкін емес.

7. Шебердің жұмысын аяқтау үшін **Нәтиже** шебер бетінде **Дайын** түймесін басыңыз.

Нәтижесінде, Kaspersky Endpoint Security for Android ұялы қолданбасының пакеті автоматты түрде Kaspersky Security Center веб-серверінде жарияланады. Ұялы қолданбалар пакетінде қолданбалар, ұялы құрылғыны Басқару сервері қосу параметрлері және сертификат бар. Ұялы құрылғының пайдаланушысы Веб-Серверден пакет жүктеуге арналған сілтемесі бар хабарландыру алады. Пайдаланушы алынған сілтемеден өз бетінше өтеді. Осыдан кейін, құрылғының операциялық жүйесі пайдаланушыдан ұялы қолданба пакетін орнатуға келісім сұрайды. Егер пайдаланушы келіссе, пакет ұялы құрылғыға жүктеледі. Пакет жүктелгеннен және Басқару серверімен синхрондалғаннан кейін, ұялы құрылғы консоль ағашының **Мобильді құрылғыларды басқару** қалтасына салынған **Ұялы құрылғылар** қалтасында көрсетіледі.

iOS MDM құрылғыларын басқару

Бұл бөлімде Kaspersky Security Center көмегімен iOS MDM құрылғыларын басқарудың қосымша мүмкіндіктері сипатталған. iOS MDM құрылғыларын басқару үшін бағдарлама келесі мүмкіндіктерді қолдайды:

- Басқарылатын iOS MDM құрылғыларының параметрлерін орталықтан конфигурациялау және конфигурациялық профильдер арқылы құрылғылардың функцияларын шектеу. Конфигурациялық профильдерді қосуға және өзгертуге және профильдерді ұялы құрылғыларға орнатуға болады.

- Provisioning профильдері арқылы App Store арқылы емес, ұялы құрылғыларға қолданбаларды орнату. Мысалы, provisioning профильдері арқылы пайдаланушылардың ұялы құрылғыларына компания ішінде жасалған корпоративтік қолданбалар орнатуға болады. Provisioning профилінде қолданба және ұялы құрылғы туралы ақпарат бар.

- Қолданбаларды App Store арқылы iOS MDM құрылғысына орнату. Қолданбаны iOS MDM құрылғысына орнатпас бұрын, қолданбаны iOS MDM серверіне қосу керек.

24 сағат сайын барлық қосылған iOS MDM құрылғыларына деректерді iOS MDM серверімен синхрондау үшін PUSH нотификациясы жіберіледі.

Конфигурациялық профиль және provisioning профилі, сондай-ақ iOS MDM құрылғысында орнатылған қолданбалар туралы ақпаратты құрылғы сипаттары терезесінде көруге болады.

iOS MDM-профиліне сертификатпен қол қою

iOS MDM профиліне сертификатпен қол қоя аласыз. Сіз өзіңіз шығарған сертификатты пайдалана аласыз немесе сенімді сертификаттау орталығынан сертификат ала аласыз.

iOS құрылғылары қол қойылмаған профильдер үшін жауапкершіліктен бас тарту туралы мәлімдемені көрсетеді және пайдаланушыға профильді орнату кезінде қол қоюшыға сенуді ұсынады.

iOS MDM профиліне сертификатпен қол қою үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

2. **Ұялы құрылғылар** қалтасының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.

3. Қалта сипаттары терезесінен **iOS құрылғыларын қосу параметрлері** бөлімін таңдаңыз.

4. **Сертификат файлын таңдау** өрісінің үстіндегі **Шолу** түймесін басыңыз.

   Сертификат терезесі ашылады.

5. **Сертификат түрі** өрісінде сертификаттың жалпыға ортақ немесе жеке түрін таңдаңыз:

   - **PKCS #12 контейнері** мәні таңдалған болса, сертификат файлы мен құпиясөзді көрсетіңіз.
   - **X.509 сертификаты** мәні таңдалған болса:

     a. жеке кілт файлын (prk немесе pem кеңейтімі бар файл) көрсетіңіз;

     b. жеке кілт құпиясөзін көрсетіңіз;

     c. жалпыға ортақ кілт файлын (cer кеңейтімі бар файл) көрсетіңіз.

6. **OK** түймесін басыңыз.

iOS MDM профиліне сертификатпен қол қойылды.

Конфигурациялық профильді қосу

Конфигурациялық профиль жасау үшін Apple Inc. веб-сайтында қолжетімді Apple Configurator 2 пайдалануға болады. Apple Configurator 2 тек macOS жүйесі бар құрылғыларда жұмыс істейді; сізде мұндай құрылғылар болмаса, оның орнына басқару консолі бар құрылғыда iPhone конфигурациялау утилитасын пайдалануға болады. Apple Inc. енді iPhone Configuration Utility қолдамайды.

iPhone Configuration Utility көмегімен конфигурациялық профильді жасау және оны iOS MDM серверіне қосу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын таңдаңыз.
2. **Мобильді құрылғыларды басқару** қалтасының жұмыс аймағында **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.
3. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.
4. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   Ұялы құрылғылар сервері сипаттары терезесі ашылады.
5. iOS MDM сервері сипаттары терезесінде **Конфигурациялық профильдер** бөлімін таңдаңыз.
6. **Конфигурациялық профильдер** бөлімінде **Жасау** түймесін басыңыз.

   Жаңа конфигурациялық профиль терезесі ашылады.
7. **Жаңа конфигурациялық профиль** терезесінде профильдің атауы мен профиль идентификаторын көрсетіңіз.

   Конфигурациялық профиль идентификаторы бірегей болуы, идентификатордың мәні Reverse-DNS пішімінде, мысалы, *com.companyname.identifier* пішімінде белгіленуі тиіс.
8. **OK** түймесін басыңыз.

   iPhone Configuration Utility бағдарламасы орнатылған болса, іске қосылады.

9. iPhone Configuration Utility бағдарламасында профиль параметрлерін конфигурациялауды орындаңыз.

   Профиль параметрлерінің сипаттамасы және оны конфигурациялау бойынша нұсқаулар iPhone Configuration Utility бағдарламасына арналған құжаттамада келтірілген.

iPhone Configuration Utility бағдарламасында профиль параметрлерін конфигурациялағаннан кейін, жаңа конфигурациялық профиль iOS MDM сервері сипаттары терезесіндегі **Конфигурациялық профильдер** бөлімінде көрсетіледі.

Өзгерту түймесі арқылы конфигурациялық профильді өңдеуге болады.

Импорттау түймесі арқылы конфигурациялық профильді бағдарламаға жүктеуге болады.

Экспорттау түймесі арқылы конфигурациялық профильді файлда сақтауға болады.

Жасалған профильді iOS MDM құрылғыларына орнату керек.

Конфигурациялық профильді құрылғыға орнату

Конфигурациялық профильді ұялы құрылғыға орнату үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында, iOS MDM құрылғыларын *iOS MDM* басқару протоколы бойынша сүзгілеңіз.

3. Конфигурациялық профильді орнату қажет болған пайдаланушының ұялы құрылғысын таңдаңыз.

   Бірнеше ұялы құрылғыны таңдап, оларға профильді бір уақытта орната аласыз.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Профильді орнату** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, сіз ұялы құрылғының контекстік мәзірінен **Барлық пәрмендер** тармағын, содан соң **Профильді орнату** тармағын таңдау арқылы пәрменді ұялы құрылғыға жібере аласыз.

   Нәтижесінде, профильдер тізімі бар **Профильдерді таңдау** терезесі ашылады. Тізімнен ұялы құрылғыға орнату қажет профильді таңдаңыз. Бірнеше профильді таңдап, ұялы құрылғыға бір уақытта орната аласыз. Профильдер ауқымын таңдау үшін **SHIFT** пәрменін қолданыңыз. Жекелеген профильдерді бір топқа біріктіру үшін **CTRL** пәрменін қолданыңыз.

6. Пәрменді ұялы құрылғыға жіберу үшін **OK** түймесін басыңыз.

   Пәрменді орындау нәтижесінде пайдаланушының ұялы құрылғысына таңдалған конфигурациялық профиль орнатылады. Пәрмен сәтті орындалған жағдайда, пәрмендер журналындағы пәрменнің ағымдағы күйі *Орындалды* мәніне ауысады.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады.

   Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

7. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

Орнатқан профиліңізді қарай аласыз және қажет болса, жоя аласыз.

Конфигурациялық профильді құрылғыдан жою

Ұялы құрылғыдан конфигурациялық профильді жою үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында, **iOS MDM** құрылғыларын iOS MDM сілтемесі бойынша сүзгілеңіз.

3. Конфигурациялық профиль жойылатын пайдаланушының ұялы құрылғысын таңдаңыз.

   Бірнеше ұялы құрылғыны таңдап, олардан профильді бір уақытта жоя аласыз.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Профильді жою** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, сіз құрылғының контекстік мәзірінен **Барлық пәрмендер**, содан соң **Профильді жою** тармағын таңдап, ұялы құрылғыға пәрмен жібере аласыз.

   Нәтижесінде, профильдер тізімі бар **Профильдер жойылуда** терезесі ашылады.

6. Тізімнен ұялы құрылғыдан жою қажет профильді таңдаңыз. Бірнеше профильді таңдап, ұялы құрылғыдан бір уақытта жоя аласыз. Профильдер ауқымын таңдау үшін **SHIFT** пәрменін қолданыңыз. Жекелеген профильдерді бір топқа біріктіру үшін **CTRL** пәрменін қолданыңыз.

7. Пәрменді ұялы құрылғыға жіберу үшін **OK** түймесін басыңыз.

   Пәрменді орындау нәтижесінде таңдалған конфигурациялық профиль пайдаланушының ұялы құрылғысынан жойылады. Пәрмен сәтті орындалған жағдайда, пәрменнің ағымдағы күйі *Аяқталды* мәніне ие болады.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады.

   Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

   Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

8. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

Профильге сілтемені жариялау арқылы жаңа құрылғыны қосу

Басқару консолінде сертификаттар орнату шеберін пайдаланып, әкімші жаңа iOS MDM профилін жасайды. Шебердің жұмысы нәтижесінде келесі әрекеттер орындалады:

- iOS MDM профилі Веб-серверде автоматты түрде жарияланады.
- Пайдаланушыға SMS-хабарда немесе электрондық пошта арқылы iOS MDM профиліне сілтеме жіберіледі. Сілтемені алғаннан кейін, пайдаланушы ұялы құрылғыда iOS MDM профилін орнатады.
- Нәтижесінде, ұялы құрылғы iOS MDM серверіне қосылады.

Apple компаниясы енгізген қауіпсіздік саясатын қатаңдатуға байланысты, iOS 11 операциялық жүйесі бар ұялы құрылғыны Public Key Infrastructure (PKI) біріктіруі конфигурацияланған Басқару серверіне қосу үшін протоколдардың TLS 1.1 және TLS 1.2 нұсқаларын конфигурациялау қажет.

Әкімшінің профильді орнатуы арқылы жаңа құрылғыны қосу

Ұялы құрылғыға iOS MDM профилін орнату арқылы ұялы құрылғыны iOS MDM серверіне қосу үшін, әкімші келесі әрекеттерді орындауы керек:

1. Басқару консолінде сертификатты орнату шеберін ашыңыз.
2. Профиль жасау шебері терезесінде **Шебердің жұмысы аяқталғаннан кейін сертификатты көрсету** жалаушасын қою арқылы жаңа iOS MDM профилін жасау.
3. iOS MDM профилін жасау.
4. Apple Configurator утилитасы арқылы пайдаланушының ұялы құрылғысына iOS MDM профилін орнату.

Нәтижесінде, ұялы құрылғы iOS MDM серверіне қосылады.

Apple компаниясы енгізген қауіпсіздік саясатын қатаңдатуға байланысты, iOS 11 операциялық жүйесі бар ұялы құрылғыны Public Key Infrastructure (PKI) біріктіруі конфигурацияланған Басқару серверіне қосу үшін протоколдардың TLS 1.1 және TLS 1.2 нұсқаларын конфигурациялау қажет.

Provisioning профилін қосу

Provisioning профилін iOS MDM серверіне қосу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын ашыңыз.
2. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.
3. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.

4. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   Ұялы құрылғылар сервері сипаттары терезесі ашылады.

5. **iOS MDM сервері** сипаттары терезесінде **Provisioning профильдері** бөліміне өтіңіз.

6. **Provisioning профильдері** бөлімінде **Импорттау** түймесін басып, provisioning профиліне апаратын жолды көрсетіңіз.

Профиль iOS MDM сервері параметрлеріне қосылады.

Экспорттау түймесі арқылы provisioning профилін файлда сақтауға болады.

Импортталған provisioning профиліңізді iOS MDM құрылғыларына орната аласыз.

Provisioning профилін құрылғыға орнату

Provisioning профилін ұялы құрылғыға орнату үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында, iOS MDM құрылғыларын *iOS MDM* басқару протоколы бойынша сүзгілеңіз.

3. Provisioning профилін орнату қажет пайдаланушының ұялы құрылғысын таңдаңыз.

   Бірнеше ұялы құрылғыны таңдап, оларға provisioning профилін бір уақытта орната аласыз.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Provisioning профилін орнату** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, сіз ұялы құрылғының контекстік мәзірінен **Барлық пәрмендер** тармағын, содан соң **Provisioning профилін орнату** тармағын таңдау арқылы пәрменді ұялы құрылғыға жібере аласыз.

   Нәтижесінде, provisioning профильдері тізімі бар **Provisioning профильдерін таңдау** терезесі ашылады. Тізімнен ұялы құрылғыға орнату қажет provisioning профилін таңдаңыз. Бірнеше provisioning профильдерін таңдап, ұялы құрылғыға бір уақытта орната аласыз. Provisioning профильдері ауқымын таңдау үшін **SHIFT** пәрменін қолданыңыз. Жекелеген provisioning профильдерін бір топқа біріктіру үшін **CTRL** пәрменін қолданыңыз.

6. Пәрменді ұялы құрылғыға жіберу үшін **OK** түймесін басыңыз.

   Пәрменді орындау нәтижесінде пайдаланушының ұялы құрылғысына таңдалған provisioning профилі орнатылады. Пәрмен сәтті орындалған жағдайда, пәрмендер журналындағы пәрменнің ағымдағы күйі *Аяқталды* мәніне ауысады.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады.

   Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

7. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

Орнатқан профиліңізді қарай аласыз және қажет болса, жоя аласыз.

Provisioning профилін құрылғыдан жою

Ұялы құрылғыдан provisioning профилін жою үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында, iOS MDM құрылғыларын *iOS MDM* басқару протоколы бойынша сүзгілеңіз.

3. Provisioning профилі жойылатын пайдаланушының ұялы құрылғысын таңдаңыз.

   Бірнеше ұялы құрылғыны таңдап, олардан provisioning профилін бір уақытта жоя аласыз.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Provisioning профилін жою** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, құрылғының контекстік мәзірінен **Барлық пәрмендер**, содан соң **Provisioning профилін жою** тармағын таңдау арқылы пәрменді ұялы құрылғыға жібере аласыз.

   Нәтижесінде, профильдер тізімі бар **Provisioning профильдерін жою** терезесі ашылады.

6. Тізімнен ұялы құрылғыдан жою қажет provisioning профилін таңдаңыз. Бірнеше provisioning профилін таңдап, ұялы құрылғыдан бір уақытта жоя аласыз. Provisioning профильдері ауқымын таңдау үшін **SHIFT** пәрменін қолданыңыз. Жекелеген provisioning профильдерін бір топқа біріктіру үшін **CTRL** пәрменін қолданыңыз.

7. Пәрменді ұялы құрылғыға жіберу үшін **OK** түймесін басыңыз.

   Пәрменді орындау нәтижесінде таңдалған provisioning профилі пайдаланушының ұялы құрылғысынан жойылады. Жойылған provisioning профилімен байланысты қолданбалар жұмыс істемейді. Пәрмен сәтті орындалған жағдайда, пәрменнің ағымдағы күйі *Аяқталды* мәніне ие болады.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады.

   Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

   Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

8. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

Басқарылатын қолданбаны қосу

Қолданбаны iOS MDM құрылғысына орнатпас бұрын, қолданбаны iOS MDM серверіне қосу керек. Қолданба Kaspersky Security Center көмегімен құрылғыға орнатылған болса, басқарылатын болып саналады. Басқарылатын қолданбаны Kaspersky Security Center құралдарымен қашықтан басқаруға болады.

iOS MDM серверіне басқарылатын қолданбаны қосу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын ашыңыз.
2. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылардың серверлері** салынған қалтасын таңдаңыз.
3. **Ұялы құрылғылардың серверлері** қалтасының жұмыс аймағында iOS MDM серверін таңдаңыз.
4. iOS MDM серверінің контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.

   iOS MDM сервері сипаттары терезесі ашылады.
5. iOS MDM сервері сипаттары терезесінде **Басқарылатын бағдарламалар** бөлімін таңдаңыз.
6. **Басқарылатын бағдарламалар** бөліміндегі **Қосу** түймесін басыңыз.

   Бағдарламаны қосу терезесі ашылады.
7. **Бағдарламаны қосу** терезесінде **Бағдарламаның атауы** өрісінде қосылатын қолданбаның атауын көрсетіңіз.
8. **Apple ID немесе манифест файлының сілтемесі** өрісінде қосылатын қолданбаның Apple идентификаторын немесе қолданбаны жүктеп алуға болатын манифест файлына сілтемені көрсетіңіз.
9. iOS MDM профилін жойған кезде пайдаланушының ұялы құрылғысынан профильмен бір уақытта басқарылатын қолданбаның да жойылғанын қаласаңыз, **iOS MDM профилімен бірге жою** жалаушасын қойыңыз.
10. Егер сіз iTunes көмегімен қолданба деректерінің сақтық көшірмесін жасағыңыз келмесе, **Деректердің сақтық көшірмесін бұғаттау** жалаушасын қойыңыз.
11. **OK** түймесін басыңыз.

Қосылған қолданба iOS MDM сервер сипаттары терезесінің **Басқарылатын бағдарламалар** бөлімінде көрсетіледі.

Қолданбаны ұялы құрылғыға орнату

Қолданбаны iOS MDM ұялы құрылғысына орнату үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.
2. Қолданбаны орнату үшін iOS MDM құрылғысын таңдаңыз.

   Қолданбаны бір уақытта орнату үшін бірнеше ұялы құрылғыларды таңдауға болады.
3. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.
4. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Қолданбаны орнату** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, сіз ұялы құрылғының контекстік мәзірінен **Барлық пәрмендер** тармағын, содан соң **Қолданбаны орнату** тармағын таңдау арқылы пәрменді ұялы құрылғыға жібере аласыз.

Нәтижесінде, профильдер тізімі бар **Қосымшаларды таңдау** терезесі ашылады. Тізімнен ұялы құрылғыға орнату қажет қолданбаны таңдаңыз. Бірнеше қолданбаны таңдап, ұялы құрылғыға бір уақытта орната аласыз. Қолданбалар ауқымын таңдау үшін **SHIFT** пәрменін қолданыңыз. Жекелеген қолданбаларды бір топқа біріктіру үшін **CTRL** пәрменін қолданыңыз.

5. Пәрменді ұялы құрылғыға жіберу үшін **OK** түймесін басыңыз.

   Пәрменді орындау нәтижесінде таңдалған қосымша пайдаланушы ұялы құрылғысына орнатылады. Пәрмен сәтті орындалған жағдайда, пәрмендер журналындағы пәрменнің ағымдағы күйі *Аяқталды* мәніне ауысады.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады. Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

   Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

6. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

Орнатылған қолданба туралы ақпарат iOS MDM ұялы құрылғысының сипаттарында көрсетіледі. Қолданбаны ұялы құрылғыдан пәрмендер журналы немесе ұялы құрылғының контекстік мәзірі арқылы жоюға болады.

Қолданбаны құрылғыдан жою

Қолданбаны ұялы құрылғыдан жою үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында, iOS MDM құрылғыларын *iOS MDM* басқару протоколы бойынша сүзгілеңіз.

3. Қолданбасын жою қажет пайдаланушының ұялы құрылғысын таңдаңыз.

   Бірнеше ұялы құрылғыны таңдап, олардан қолданбаны бір уақытта жоя аласыз.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Қолданбаны жою** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, сіз ұялы құрылғының контекстік мәзірінен **Барлық пәрмендер** тармағын, содан соң **Бағдарламаны жою** тармағын таңдау арқылы пәрменді ұялы құрылғыға жібере аласыз.

   Нәтижесінде, қолданбалар тізімі бар **Қосымшалар жойылуда** терезесі ашылады.

6. Тізімнен ұялы құрылғыдан жою қажет қолданбаны таңдаңыз. Бірнеше қолданбаны таңдап, құрылғыдан бір уақытта жоя аласыз. Қолданбалар ауқымын таңдау үшін **SHIFT** пәрменін қолданыңыз. Жекелеген қолданбаларды бір топқа біріктіру үшін **CTRL** пәрменін қолданыңыз.

7. Пәрменді ұялы құрылғыға жіберу үшін **OK** түймесін басыңыз.

   Пәрменді орындау нәтижесінде таңдалған қосымша пайдаланушының ұялы құрылғысынан жойылады. Пәрмен сәтті орындалған жағдайда, пәрменнің ағымдағы күйі *Аяқталды* мәніне ие болады.

   Қайтадан жіберу түймесі бойынша пәрменді пайдаланушының ұялы құрылғысына тағы да бір рет жіберуге болады.

   Пәрмен әлі орындалмаған болса, **Кезектен жою** түймесі арқылы, жіберілген пәрменнің орындалуын болдырмауға болады.

Пәрмендер журналы бөлімі мобильдік құрылғыға жіберілген пәрмендерді сәйкес орындалу күйлерімен көрсетеді. Пәрмендер тізімін жаңарту үшін **Жаңарту** түймесін басыңыз.

8. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесін жабу үшін **OK** түймесін басыңыз.

iOS MDM ұялы құрылғысында роуминг параметрлерін конфигурациялау

Роуминг параметрлерін теңшеу үшін:

1. Консоль ағашында **Мобильді құрылғыларды басқару** қалтасын ашыңыз.
2. **Мобильді құрылғыларды басқару** қалтасында **Ұялы құрылғылар** ішкі қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.
3. Роумингті конфигурациялау үшін пайдаланушының iOS MDM құрылғысын таңдаңыз.

   Роумингті бір уақытта конфигурациялау үшін бірнеше ұялы құрылғыларды таңдауға болады.
4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.
5. **Ұялы құрылғыларды басқаруға арналған пәрмендер** терезесінде **Роуминг параметрлерін теңшеу** бөліміне өтіп, **Пәрмен жіберу** түймесін басыңыз.

   Сондай-ақ, сіз құрылғының контекстік мәзірінен **Барлық пәрмендер → Роуминг параметрлерін теңшеу** тармағын таңдап, ұялы құрылғыға пәрмен жібере аласыз.
6. **Роуминг параметрлері** терезесінде өзіңізге қажетті параметрлерді көрсетіңіз:

   - **Деректер роумингін қосу**

     Егер параметр қосулы болса, iOS MDM ұялы құрылғысында роуминг қосулы. iOS MDM құрылғылары пайдаланушысы роумингте интернетті қолдана алады.

     Әдепкі бойынша, параметр өшірулі.

Роуминг параметрлері таңдалған құрылғылар үшін конфигурацияланған.

iOS MDM құрылғысы туралы ақпаратты қарау

iOS MDM құрылғысы туралы ақпаратты қарау үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.
2. Жұмыс аймағында, **iOS MDM** құрылғыларын iOS MDM сілтемесі бойынша сүзгілеңіз.
3. Ақпаратты қарау керек ұялы құрылғыны таңдаңыз.
4. Ұялы құрылғының контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Нәтижесінде, iOS MDM құрылғысы сипаттары терезесі ашылады.

Ұялы құрылғының сипаттары терезесінде қосылған iOS MDM құрылғысы туралы ақпарат көрсетіледі.

iOS MDM құрылғысын басқарудан өшіру

iOS MDM құрылғысын iOS MDM серверінен ажырату үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында, **iOS MDM** құрылғыларын iOS MDM сілтемесі бойынша сүзгілеңіз.

3. Өшіру керек ұялы құрылғыны таңдаңыз.

4. Ұялы құрылғының контекстік мәзірінде **Жою** тармағын таңдаңыз.

   Нәтижесінде, iOS MDM құрылғысы жою тізімінде белгіленеді. Ұялы құрылғы iOS MDM серверінің дерекқорынан жойылғаннан кейін басқарылатын құрылғылар тізімінен автоматты түрде жойылады. Ұялы құрылғыны iOS MDM серверінің дерекқорынан жою бір минут ішінде жүзеге асырылады.

iOS MDM құрылғысын ұялы құрылғыдан басқарудан ажырату нәтижесінде барлық орнатылған конфигурациялық профильдер, iOS MDM профилі және **iOS MDM профилімен бірге жою** параметрі таңдалған қолданбалар жойылады.

Құрылғыға пәрмендерді жіберу

iOS MDM құрылғысына пәрменді жіберу үшін:

1. Басқару консолінде **Мобильді құрылғыларды басқару** түйінін орналастырыңыз.

2. **Ұялы құрылғылар** қалтасын таңдаңыз.

3. **Ұялы құрылғылар** қалтасында пәрмендер жіберілетін ұялы құрылғыны таңдау.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

5. Қалқымалы тізімде, ұялы құрылғыға жіберілетін қажетті пәрменді таңдаңыз.

Жіберілген пәрмендерді орындау күйін тексеру

Ұялы құрылғыға жіберілген пәрменнің орындалу күйін тексеру үшін:

1. Басқару консолінде **Мобильді құрылғыларды басқару** түйінін орналастырыңыз.

2. **Ұялы құрылғылар** қалтасын таңдаңыз.

3. **Ұялы құрылғылар** қалтасында жіберілген пәрмендердің орындалу күйін тексеру қажет ұялы құрылғыны таңдаңыз.

4. Ұялы құрылғының контекстік мәзірінде **Пәрмендер журналын көрсету** тармағын таңдаңыз.

KES құрылғыларын басқару

Kaspersky Security Center бағдарламасында сіз KES құрылғыларын келесі жолдармен басқара аласыз:

- KES құрылғыларын пәрмендер арқылы орталықтандырылған түрде басқару;
- KES құрылғыларын басқару параметрлері туралы ақпаратты қарау;
- қолданбаларды ұялы қолданбалар пакеттері арқылы орнату;
- KES құрылғыларын басқарудан ажырату.

KES құрылғыларына арналған ұялы қолданбалар пакетін жасау

KES құрылғыларына арналған ұялы қолданбалар пакетін жасау үшін Kaspersky Endpoint Security for Android лицензиясы қажет.

Ұялы қолданбалар пакетін жасау үшін:

1. **Қашықтан орнату** қалтасындағы консоль шежіресінен **Орнату пакеттері** салынған қалтасын таңдаңыз.

   Қашықтан орнату қалтасы әдепкі бойынша **Кеңейтілген** қалтасына салынған.

2. **Қосымша әрекеттер** түймесін басыңыз да, ашылатын тізімнен **Ұялы қолданбалар пакеттерін басқару** мәнін таңдаңыз.

3. **Ұялы қолданбалар пакетін басқару** терезесінде **Жаңа** түймесін басыңыз.

4. Орнату пакетін жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Жасалған ұялы қолданбалар пакеті **Ұялы қолданбалар пакетін басқару** терезесінде көрсетіледі.

KES құрылғыларының сертификаттары негізінде түпнұсқалықты тексеруді қосу

KES құрылғыларының сертификаттары негізінде түпнұсқалықты тексеруді қосу үшін:

1. Басқару сервері орнатылған клиент құрылғысының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.

2. Келесі бөлімге өтіңіз:

   - 32 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - 64 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. LP_MobileMustUseTwoWayAuthOnPort13292 атты кілт жасаңыз.

4. REG_DWORD кілт түрін көрсетіңіз.

5. 1 кілт мәнін белгілеңіз.

6. Басқару сервері қызметін қайта іске қосыңыз.

Нәтижесінде, жалпы сертификатты қолдану арқылы KES құрылғысының сертификаттары негізінде түпнұсқалықты міндетті түрде тексеру, Басқару сервері қызметі іске қосылғаннан кейін қосылатын болады.

KES құрылғысын Басқару серверіне бірінші рет қосқан кезде сертификаттың болуы маңызды емес.

Әдепкі бойынша, KES құрылғыларының сертификаттары негізінде түпнұсқалықты тексеру мүмкіндігі ажыратылған.

KES құрылғысы туралы ақпаратты қарау

KES құрылғысы туралы ақпаратты қарау үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында KES құрылғыларын *KES* басқару протоколы бойынша сүзгілеңіз.

3. Ақпаратты қарау керек ұялы құрылғыны таңдаңыз.

4. Ұялы құрылғының контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

Нәтижесінде, KES құрылғысы сипаттары терезесі ашылады.

Ұялы құрылғы сипаттары терезесінде қосылған KES құрылғысы туралы ақпарат көрсетіледі.

KES құрылғыларын басқарудан ажырату

KES құрылғысын басқарудан ажырату үшін пайдаланушы Желілік агентті ұялы құрылғыдан жоюы керек. Пайдаланушы Желілік агентті жойғаннан кейін, ұялы құрылғы туралы ақпарат Басқару сервері дерекқорынан жойылады және әкімші ұялы құрылғыны басқарылатын құрылғылар тізімінен жоя алады.

KES құрылғысын басқарылатын құрылғылар тізімінен жою үшін:

1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Ұялы құрылғылар** салынған қалтасын таңдаңыз.

   Қалтаның жұмыс аймағында басқарылатын ұялы құрылғылардың тізімі көрсетіледі.

2. Жұмыс аймағында KES құрылғыларын *KES* басқару протоколы бойынша сүзгілеңіз.

3. Басқарудан өшіру керек ұялы құрылғыны таңдаңыз.

4. Ұялы құрылғының контекстік мәзірінде **Жою** тармағын таңдаңыз.

Нәтижесінде, ұялы құрылғы басқарылатын құрылғылар тізімінен жойылады.

Kaspersky Endpoint Security for Android қолданбасы ұялы құрылғыдан жойылмаса, онда Басқару серверімен синхрондалғаннан кейін ұялы құрылғы қайтадан басқарылатын құрылғылар тізімінде пайда болады.

Деректерді шифрлау және қорғау

Деректерді шифрлау, портативті құрылғыны, алынбалы жетекті немесе қатты дискіні ұрлаған/жоғалтқан жағдайда немесе деректерге авторизацияланбаған пайдаланушылар мен бағдарламалар қатынасқан жағдайда ақпараттың абайсызда ағып кету қаупін азайтады.

Kaspersky Endpoint Security for Windows бағдарламасында шифрлау іске асырылған. Kaspersky Endpoint Security for Windows құрылғылардың жергілікті дискілерінде және алынбалы жетектерде сақталатын файлдарды, алынбалы жетектерді және қатты дискілерді толығымен шифрлауға мүмкіндік береді.

Шифрлау ережелерін конфигурациялау, саясатты анықтау арқылы Kaspersky Security Center көмегімен жүзеге асырылады. Белгіленген ережелер бойынша шифрлау және шифрсыздау саясатты қолдану кезінде орындалады.

Шифрлауды басқару функционалдылығының қолжетімділігі пайдаланушы интерфейсінің параметрлері тарапынан анықталады.

Әкімші келесі әрекеттерді орындай алады:

- құрылғының жергілікті дискілеріндегі файлдарды шифрлауды немесе шифрсыздауды конфигурациялау және орындау;
- алынбалы жетектердегі файлдарды конфигурациялау және шифрлау;
- бағдарламалардың шифрланған файлдарға қатынасу ережелерін қалыптастыру;
- егер пайдаланушы құрылғысында файлдарды шифрлау мүмкіндігі шектеулі болса, шифрланған файлдарға қатынасу кілті файлын жасаңыз және пайдаланушыға жіберіңіз;
- қатты дискілерді конфигурациялау және шифрлау;
- пайдаланушылардың шифрланған қатты дискілерге және алынбалы жетектерге қатынасуын басқару (түпнұсқалық растама агентінің есептік жазбаларын басқару, пайдаланушыларға есептік жазбаның атауы мен құпиясөзін қалпына келтіру сұрауына жауап блоктарын және шифрланған құрылғыларға қатынасу кілттерін қалыптастыру және беру);
- шифрлау күйлері мен файлдарды шифрлау туралы есептерді қараңыз.

Бұл операциялар Kaspersky Endpoint Security for Windows бағдарламасының құралдарымен орындалады. Операцияларды орындау бойынша толығырақ нұсқаулар және шифрлау ерекшеліктерінің сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

Kaspersky Security Center бағдарламасы macOS операциялық жүйелері бар құрылғылар үшін шифрлауды басқару функционалын қолдайды. Шифрлауды конфигурациялау, шифрлауды қолдайтын бағдарламалардың нұсқалары үшін Kaspersky Endpoint Security for Mac бағдарламасының көмегімен жүзеге асырылады. Операцияларды орындау бойынша толығырақ нұсқаулар және шифрлау ерекшеліктерінің сипаттамасы *Kaspersky Endpoint Security for Mac Әкімші нұсқаулығында* келтірілген.

Шифрланған құрылғылар тізімін қарау

Ақпараты шифрланған құрылғылардың тізімін көру үшін:

1. Басқару сервері консолі ағашында **Деректерді шифрлау және қорғау** қалтасын таңдаңыз.
2. Келесі тәсілдердің бірімен шифрланған құрылғылар тізіміне өтіңіз:
   - **Шифрланған құрылғылар тізіміне өту** сілтемесі бойынша **Шифрланған құрылғыларды басқару** бөліміне өтіңіз.
   - Консоль ағашында **Шифрланған құрылғы** қалтасын таңдаңыз.

Нәтижесінде, жұмыс аймағында шифрланған файлдары бар желідегі құрылғылар және диск деңгейінде шифрланған құрылғылар туралы ақпарат ұсынылады. Құрылғыдағы ақпарат шифрсызданғаннан кейін, құрылғы тізімнен автоматты түрде жойылады.

Құрылғылар тізіміндегі ақпаратты кез келген бағанның деректерінің өсуі немесе азаюы бойынша сұрыптауға болады.

Консоль ағашында **Деректерді шифрлау және қорғау** қалтасының болуы немесе болмауы Деректерді шифрлау және қорғау тарапынан анықталады.

Шифрлау оқиғалары тізімін қарау

Kaspersky Endpoint Security for Windows құрылғыларындағы деректерді шифрлау немесе шифрсыздау тапсырмаларын орындау барысында Kaspersky Security Center бағдарламасына келесі типтегі оқиғалар туралы ақпарат жібереді:

- Дискідегі орынның жетіспеушілігіне байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес.
- Лицензиямен байланысты мәселелерге байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес.
- Қатынасу құқықтарының болмауына байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес.
- Қолданбаға шифрланған файлға кіруге тыйым салынды.
- Белгісіз қателер.

Құрылғыларда деректерді шифрлау кезінде туындаған оқиғалар тізімін қарап шығу үшін:

1. Басқару сервері консолі ағашында **Деректерді шифрлау және қорғау** қалтасын таңдаңыз.
2. Келесі тәсілдердің бірімен шифрлау кезінде орын алған оқиғалар тізіміне өтіңіз:
   - **Қателер тізіміне өту** сілтемесі бойынша **Деректерді шифрлау қателері** бөліміне өтіңіз.
   - Консоль ағашында **Шифрланған құрылғы** қалтасын таңдаңыз.

Нәтижесінде, жұмыс аймағында құрылғылардағы деректерді шифрлау кезінде туындаған мәселелер туралы ақпарат беріледі.

Шифрлау оқиғаларының тізімімен келесі әрекеттерді орындауға болады:

- жазбаларды кез келген бағандағы деректердің өсуі немесе азаюы бойынша сұрыптау;
- жазбалар бойынша жылдам іздеу (кез келген тізім өрісіндегі ішкі жолға сәйкес мәтіндік сәйкестік бойынша);
- құрылған оқиғалар тізімін мәтіндік файлға экспорттау.

Консоль ағашында **Деректерді шифрлау және қорғау** қалтасының болуы немесе болмауы Деректерді шифрлау және қорғау тарапынан анықталады.

Шифрлау оқиғаларының тізімін мәтіндік файлға экспорттау

Шифрлау оқиғаларының тізімін мәтіндік файлға экспорттау үшін:

1. Шифрлау оқиғалары тізімін қалыптастырыңыз.
2. Оқиғалар тізімінің контекстік мәзірінен **Тізімді экспорттау** тармағын таңдаңыз.

   Тізімді экспорттау терезесі ашылады.
3. **Тізімді экспорттау** терезесінде, оқиғалар тізімі бар мәтіндік файл атауын көрсетіңіз, ол сақталатын қалтаны таңдаңыз және **Сақтау** түймесін басыңыз.

   Шифрлау оқиғаларының тізімі көрсетілген файлға сақталады.

Шифрлау туралы есептерді қалыптастыру және қарау

Сіз келесі есептерді құрастыра аласыз:

- Басқарылатын құрылғыларды шифрлаудың күйі туралы есеп. Бұл есепте түрлі басқарылатын құрылғылардың деректерін шифрлау туралы мәлімет көрсетілген. Мысалы, есепте конфигурацияланған шифрлау ережелері бар саясат қолданылатын құрылғылардың саны көрсетілген. Сондай-ақ, мысалы, қанша құрылғыны қайта іске қосу керектігін білуге болады. Сондай-ақ, есепте әрбір құрылғы үшін шифрлау технологиясы мен алгоритмі туралы ақпарат қамтылған.

- Жаппай сақтау құрылғыларының шифрлау күйлері туралы есеп беру. Бұл есеп, басқарылатын құрылғыларды шифрлау күйі туралы есепке ұқсас ақпаратты қамтиды, бірақ деректерді тек жаппай сақтау құрылғыларына және алынбалы жетектерге ғана ұсынады.

- Шифрланған құрылғыға қатынасу құқықтары туралы есеп. Бұл есеп шифрланған қатты дискіге қандай пайдаланушы есептік жазбалары кіретінін көрсетеді.

- Файлдарды шифрлау қателері туралы есеп. Есепте құрылғылардағы деректерді шифрлау немесе шифрсыздау тапсырмаларын орындау кезінде пайда болған қателер туралы ақпарат бар.

- Шифрланған файлдарға қатынасты бұғаттау туралы есеп. Есепте бағдарламалардың шифрланған файлдарға қатынасуын бұғаттау туралы ақпарат бар. Бұл есеп, авторизацияланбаған пайдаланушы немесе бағдарлама шифрланған файлдарға немесе қатты дискілерге қатынас алуға әрекеттеніп жатса, пайдалы болады.

Құрылғыларды шифрлау есебін құрастыру үшін:

1. Консоль ағашында **Деректерді шифрлау және қорғау** қалтасын таңдаңыз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Басқарылатын құрылғыларды шифрлаудың күйі туралы есепті құрастыру үшін **Жаппай сақтау құрылғыларын шифрлау күйі туралы есепті көру** сілтемесінен өтіңіз.

     Есеп бұған дейін конфигурацияланбаған болса, есеп үлгісін жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

   - Жаппай сақтау құрылғыларының шифрлау күйлері туралы есепті құрастыру үшін, консоль ағашында **Шифрланған құрылғы** ішкі қалтасын таңдап, **Жаппай сақтау құрылғыларын шифрлау күйі туралы есепті көру** түймесін басыңыз.

Есепті іске қосу процесі басталады. Есеп **Басқару сервері** түйінінің **Есептер** қойындысында пайда болады.

Шифрланған құрылғыларға қатынасу құқығы туралы есепті қалыптастыру үшін:

1. Консоль ағашында **Деректерді шифрлау және қорғау** қалтасын таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:
   - **Шифрланған құрылғыларды басқару** блогындағы **Шифрланған құрылғыға қатынасу құқықтары туралы есеп** сілтемесі бойынша есеп үлгісін жасау шеберін іске қосыңыз.
   - **Шифрланған құрылғы** салынған қалтасын таңдаңыз, содан соң **Шифрланған құрылғыға қатынасу құқықтары туралы есеп** түймесін басып есеп үлгісін жасау шеберін іске қосыңыз.
3. Есеп үлгісін жасау шебері қадамдарын орындаңыз.

Есепті іске қосу процесі басталады. Есеп **Басқару сервері** түйінінің **Есептер** қойындысында пайда болады.

Файлдарды шифрлау қателері туралы есепті құрастыру үшін:

1. Консоль ағашында **Деректерді шифрлау және қорғау** қалтасын таңдаңыз.
2. Келесі әрекеттердің бірін орындаңыз:
   - **Деректерді шифрлау қателері** басқару блогында **Файлдарды шифрлау қателері туралы есепті көру** сілтемесі бойынша есеп үлгісін жасау шеберін іске қосыңыз.
   - **Шифрлау оқиғалары** салынған қалтасын таңдап, **Файлдарды шифрлау қателері туралы есеп** сілтемесі бойынша есеп үлгісін жасау шеберін іске қосыңыз.
3. Есеп үлгісін жасау шебері қадамдарын орындаңыз.

Есепті іске қосу процесі басталады. Есеп **Басқару сервері** түйінінің **Есептер** қойындысында пайда болады.

Басқарылатын құрылғыларды шифрлаудың күйі туралы есепті құрастыру үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. **Жаңа есеп үлгісі** түймесі арқылы есеп үлгісін жасау шеберін іске қосыңыз.
4. Есеп үлгісін жасау шеберінің нұсқауларын орындаңыз. **Есеп үлгісінің түрін таңдау** терезесі, **Басқа** бөлімінде **Басқарылатын құрылғыларды шифрлаудың күйі туралы есепті** таңдаңыз.

   Есеп үлгісін жасау шеберінің жұмысы аяқталғаннан кейін, Басқару сервері түйінінде, **Есептер** қойыншасында жаңа есеп үлгісі пайда болады.
5. Қажетті Басқару серверінің түйінінде **Есептер** қойыншасында нұсқаулықтың алдыңғы қадамдарында жасалған есеп үлгісін таңдаңыз.

Есепті іске қосу процесі басталады. Есеп **Басқару сервері** түйінінің **Есептер** қойындысында пайда болады.

Құрылғылардың шифрлау күйлері мен алынбалы жетектердің шифрлау саясатына сәйкестігі туралы ақпаратты Басқару сервері түйінінің **Статистика** қойыншасындағы ақпараттық тақталардан да көруге болады.

Шифрланған файлдарға қатынасты бұғаттау туралы есепті құрастыру үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.
2. Тораптың жұмыс аймағында **Есептер** қойыншасын таңдаңыз.
3. **Жаңа есеп үлгісі** түймесі бойынша есеп үлгісін жасау шеберін іске қосыңыз.
4. Есеп үлгісін жасау шеберінің нұсқауларын орындаңыз. **Есеп үлгісінің түрін таңдау** терезесінде, **Басқа** бөлімінде **Шифрланған файлдарға қатынасты бұғаттау туралы есеп** тармағын таңдаңыз.

   Есеп үлгісін жасау шеберінің жұмысы аяқталғаннан кейін, **Басқару сервері** түйінінде, **Есептер** қойыншасында жаңа есеп үлгісі пайда болады.
5. **Басқару сервері** түйінінде **Есептер** қойыншасында нұсқаулықтың алдыңғы қадамдарында жасалған есеп үлгісін таңдаңыз.

Есепті іске қосу процесі басталады. Есеп **Басқару сервері** түйінінің **Есептер** қойындысында пайда болады.

Басқару серверлері арасында шифрлау кілттерін беру

Егер басқарылатын құрылғыда деректерді шифрлау функциясы қосылса, шифрлау кілті Басқару серверінде сақталады. Шифрлау кілті шифрланған деректерге қол жеткізу және шифрлау саясатын басқару үшін қолданылады.

Шифрлау кілті келесі жағдайларда басқа Басқару серверіне берілуі керек:

- Құрылғыны басқа Басқару серверіне тағайындау үшін басқарылатын құрылғыда Желілік агентті қайта конфигурацияладыңыз. Егер бұл құрылғыда шифрланған деректер болса, шифрлау кілті мақсатты Басқару серверіне берілуі керек. Әйтпесе, деректерді шифрсыздау мүмкін болмайды.
- Сіз S1 Басқару сервері басқаратын D1 құрылғысына қосылған алынбалы дискіні шифрладыңыз, содан кейін бұл алынбалы дискіні S2 Басқару сервері басқаратын D2 құрылғысына қосасыз. Алынбалы дискідегі деректерге қол жеткізу үшін шифрлау кілті S1 Басқару серверінен S2 Басқару серверіне берілуі керек.
- Сіз файлды S1 Басқару сервері басқаратын D1 құрылғысында шифрладыңыз, содан кейін S2 Басқару сервері басқаратын D2 құрылғысында файлға қатынасу мүмкіндігін алуға тырысасыз. Файлға қол жеткізу үшін шифрлау кілті S1 Басқару серверінен S2 Басқару серверіне берілуі керек.

Шифрлау кілттерін келесі тәсілдермен беруге болады:

- Автоматты түрде, шифрлау кілті берілуі тиісті екі Басқару серверінің сипаттарында **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрін қосу арқылы. Егер бұл параметр Басқару серверлерінің бірі үшін өшірулі болса, шифрлау кілттерін автоматты түрде беру мүмкін емес.

  Басқару сервері сипаттарында **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрін қосқанда, Басқару сервері шифрлау кілттерін негізгі Басқару серверіне (егер бар болса) жоғарыдағы иерархияның бір деңгейіне жібереді.

Шифрланған деректерге қатынасуға тырысқанда, Басқару сервері алдымен өз қоймасынан шифрлау кілтін іздейді. Егер **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрі қосулы болса және қажетті шифрлау кілті қоймада болмаса, Басқару сервері қажетті шифрлау кілтін алу үшін негізгі Басқару серверіне (егер бар болса) қосымша сұрау жібереді. Сұрау иерархияның ең жоғарғы деңгейіндегі Серверге дейін барлық негізгі Басқару серверлеріне жіберіледі.

Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану параметрі Web Console интерфейсінде қолжетімді емес. MMC негізіндегі басқару консоліне кіру мүмкіндігіңіз болмаса, шифрланған құрылғыларды басқару үшін негізгі басқару серверін пайдаланыңыз.

- Шифрлау кілттері бар файлды экспорттау және импорттау арқылы, бір Басқару серверінен екіншісіне қолмен.

  Шифрлау кілттерін экспорттау және импорттау – бұл шифрлау кілттерін басқару функционалына кіретін әрекеттер. Осы қадамдарды орындау мақсатында, Kaspersky Security Center пайдаланушылары үшін функцияға қатынасу құқығын келесідей конфигурациялаңыз:

  - Шифрлау кілттерін қосалқы Басқару серверінен экспорттайтын пайдаланушы үшін Шифрлау кілтін басқару функциясына **Оқу** құқығын беру.
  - Қажетті Басқару серверіне шифрлау кілттерін импорттайтын пайдаланушы үшін Шифрлау кілтін басқару функциясына **Жазу** құқығын беру.

Иерархиядағы Басқару серверлері арасында шифрлау кілттерін автоматты түрде беруді қосу үшін:

1. Консоль ағашында шифрлау кілттерін автоматты түрде беруді қосатын Басқару серверін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Сипаттар терезесінен **Шифрлау алгоритмі** бөлімін таңдаңыз.
4. **Шифрлау кілттерін алу үшін Басқару серверлерінің иерархиясын пайдалану** параметрін қосыңыз.
5. Өзгерістерді қолдану үшін **OK** түймесін басыңыз.

Шифрлау кілттері келесі синхрондау кезінде (жүрек соғу жиілігі пакеті) негізгі Басқару серверіне (егер бар болса) жіберіледі. Бұл Басқару сервері, сұрау бойынша қосалқы Басқару серверіне өз қоймасынан шифрлау кілтін де ұсынады.

Басқару серверлері арасында шифрлау кілттерін қолмен беру үшін:

1. Басқару сервері консолі ағашында шифрлау кілттерін тасымалдауды қажет ететін қосалқы Басқару серверін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Сипаттар терезесінен **Шифрлау алгоритмі** бөлімін таңдаңыз.
4. **Басқару серверінен шифрлау кілттерін экспорттау** түймесін басыңыз.

   Серверден шифрлау кілттерін экспорттайтын пайдаланушыға Шифрлау кілтін басқару функциясына **Оқу** құқығы берілгеніне көз жеткізіңіз.

5. **Шифрлау кілттерін экспорттау** терезесінде:

   - **Шолу** түймесін басыңыз, содан соң файлды қайда сақтау керектігін көрсетіңіз.
   - Файлды рұқсатсыз қатынасудан қорғау үшін құпиясөзді енгізіңіз.

   > Құпиясөзді еске сақтаңыз. Жоғалған құпиясөзді қалпына келтіру мүмкін емес. Егер құпиясөз жоғалса, экспорттау процедурасын қайталау қажет. Сондықтан, құпиясөзді жазып алып, жақын жерде ұстаңыз.

6. Файлды басқа Басқару серверіне жіберіңіз, мысалы, ортақ қатынасы бар қалта немесе алынбалы жетек арқылы.
7. Мақсатты Басқару серверінде Kaspersky Security Center Басқару консолі жұмыс істеп тұрғанына көз жеткізіңіз.
8. Басқару сервері консолі ағашында шифрлау кілттерін тасымалдауды қажет ететін мақсатты Басқару серверін таңдаңыз.
9. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
10. Сипаттар терезесінен **Шифрлау алгоритмі** бөлімін таңдаңыз.
11. **Басқару серверіне шифрлау кілттерін импорттау** түймесін басыңыз.

    Серверге шифрлау кілттерін импорттайтын пайдаланушыға **Шифрлау кілтін басқару функциясына** Жазу құқығы берілгеніне көз жеткізіңіз.
12. **Шифрлау кілттерін импорттау** терезесінде:

    - **Шолу** түймесін басып, шифрлау кілттерін қамтитын файлды таңдаңыз.
    - Құпиясөзді көрсетіңіз.
13. **ОК** түймесін басыңыз.

Шифрлау кілттері мақсатты Басқару серверіне жіберіледі.

Деректер қоймасы

Бұл бөлімде Басқару серверінде сақталатын және клиент құрылғыларының күйін бақылау және оларға қызмет көрсету үшін пайдаланылатын мәліметтер туралы ақпарат бар.

Клиент құрылғылардың күйін бақылау және оларға қызмет көрсету үшін пайдаланылатын деректер консоль ағашының **Қоймалар** қалтасында көрсетіледі.

Қоймалар қалтасы келесі нысандарды қамтиды:

- клиент құрылғыларына таралатын Басқару сервері жүктеген жаңартулар;
- желіде табылған жабдықтардың тізімі;
- клиент құрылғыларында табылған лицензиялық кілттер;

- қауіпсіздік бағдарламалары құрылғылардағы карантиндік қалталарға орналастырған файлдар;
- клиент құрылғылардың резервтік қоймаларына орналастырылған файлдар;
- қауіпсіздік бағдарламалары кейінге қалдырылған тексерудің қажеттілігін анықтаған файлдар.

Қоймадағы нысандар тізімін мәтіндік файлға экспорттау

Сіз мәтіндік файлға қоймадағы нысандардың тізімін экспорттай аласыз.

Мәтіндік файлға қоймадағы нысандардың тізімін экспорттау үшін:

1. **Қоймалар** қалтасындағы консоль ағашында өзіңізге қажетті салынған қалтаны таңдаңыз.
2. Сақтау нысандары тізімінің контекстік мәзірінен **Тізімді экспорттау** тармағын таңдаңыз.

   Нәтижесінде, **Тізімді экспорттау** терезесі ашылып, онда сіз контекстік файлдың атауын және ол орналастырылатын қалтаның мекенжайын көрсете аласыз.

Орнату пакеттері

Kaspersky Security Center деректер қоймаларына Kaspersky бағдарламаларының және үшінші тарап бағдарламаларының орнату пакеттерін орналастырады.

Орнату пакеті – бағдарламаны орнатуға қажетті файлдар жиынтығы. Орнату пакетінде орнату процесінің параметрлері және орнатылатын бағдарламаның бастапқы конфигурациясы бар.

Егер сіз клиент құрылғысына қандай да бір бағдарламаны орнатқыңыз келсе, бұл бағдарлама үшін орнату пакетін жасау немесе бұрыннан жасалған орнату пакетін пайдалану қажет. Жасалған орнату пакеттері тізімі **Қашықтан орнату** консоль ағашы қалтасында, **Орнату пакеттері** салынған қалтасында сақталады.

Қоймадағы файлдардың негізгі күйлері

Қауіпсіздік бағдарламалары құрылғылардағы файлдарды белгілі вирустар мен басқа қауіп төндіретін бағдарламалардың бар-жоғы тұрғысынан тексереді, файлдарға күй тағайындайды және кейбір файлдарды қоймаға орналастырады.

Мысалы, қауіпсіздік бағдарламалары келесіні жасай алады:

- файлды жоюдың алдында, оның көшірмесін қоймаға сақтай алады;
- вирус жұққан болуы мүмкін файлдарды қоймада оқшаулай алады.

Файлдардың негізгі күйлері төмендегі кестеде келтірілген. Қауіпсіздік бағдарламаларының анықтамалықтарындағы файлдармен жасалатын әрекеттер туралы толығырақ ақпаратты ала аласыз.

Күйдің атауы	Күйдің сипаттамасы
Вирус жұққан	Файлда, Kaspersky антивирустық дерекқорларында ақпараты бар белгілі вирус кодының немесе басқа қауіп төндіретін бағдарламаның аумағы табылды.
Вирус жұқпаған	Файлда белгілі вирустар немесе қауіп төндіретін басқа зиянды бағдарламалар табылған жоқ.
Ескерту	Файлда белгілі қауіп кодының бақылау аумағына ішінара сәйкес келетін код аумағы бар.
Вирус жұққан болуы мүмкін	Файлда белгілі вирустың түрлендірілген коды немесе Kaspersky бағдарламасына әлі белгісіз вирусқа ұқсайтын код бар.
Қалтаға пайдаланушы орналастырған	Пайдаланушы файлды өз бетінше қоймаға орналастырды, мысалы, файлдың әрекеті оған қауіп төндіреді деп күдіктенуге негіз болды. Пайдаланушы жаңартылған дерекқорлар арқылы файлдағы қауіптердің бар-жоғын тексере алады.
Жалған іске қосылу	Kaspersky бағдарламасы вирус кодына ұқсайтындығына байланысты вирус жұқпаған файлға вирус жұққан күйін берді. Жаңартылған дерекқорларды пайдаланып тексергеннен кейін, файл вирус жұқтырмаған деп анықталады.
Емделді	Файлды емдеу мүмкін болмады.
Жойылды	Файл өңдеу нәтижесінде жойылды.
Құпиясөзбен қорғалған	Файл құпиясөзбен қорғалғандықтан, өңделе алмайды.

Ережелердің Смарт оқыту режимінде іске қосылуы

Бұл бөлімде клиент құрылғыларындағы Kaspersky Endpoint Security for Windows Аномалияларды бейімделумен басқару ережелері орындаған анықтаулар туралы ақпарат берілген.

Ережелер клиент құрылғыларындағы қалыптан тыс жүріс-тұрысты анықтайды және оны бұғаттай алады. Егер ережелер Смарт оқыту режимінде жұмыс істесе, олар қалыптан тыс мінез-құлықты анықтайды және әрбір осындай жағдай туралы есептерді Kaspersky Security Center Басқару серверіне жібереді. Бұл ақпарат **Қоймалар** қалтасына салынған **"Смарт оқыту" күйіндегі ереже триггерлері** қалтасында тізім түрінде сақталады. Сіз анықтауды дұрыс деп растай аласыз немесе оны ерекшеліктерге қоса аласыз, содан кейін жүріс-тұрыстың бұл түрі қалыптан тыс болып саналмайды.

Анықтау туралы ақпарат Басқару серверіндегі оқиғалар журналында (қалған оқиғалармен бірге) және Аномалияларды бейімделумен басқару есебінде сақталады.

Аномалияларды бейімделумен басқару, оның ережелері, олардың режимдері мен күйлері туралы толық ақпарат Kaspersky Endpoint Security for Windows анықтамасында берілген.

Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау тізімін қарау

Аномалияларды бейімделумен басқару ережелері арқылы орындалған анықтау тізімін қарау үшін:

1. Консоль ағашында Басқару серверінің қажетті түйінін таңдаңыз.

2. **"Смарт оқыту" күйіндегі ереже триггерлері** ішкі қалтасын таңдаңыз (әдепкі бойынша ол **Кеңейтілген** → **Қоймалар** қалтасында орналасқан).

   Тізімде Аномалияларды бейімделумен басқару ережелері арқылы орындалатын келесі анықтау ақпарат көрсетіледі:

   - **Басқару тобы**

     Құрылғы қосылған басқару тобының атауы.

- **Құрылғы атауы**

  Ереже қолданылған клиент құрылғысының атауы.

- **Атауы**

  Қолданылған ереже атауы.

- **Күйі**

  Ерекшелік – егер әкімші бұл анықтауды өңдеп, оны ережелерден ерекшелік ретінде қосқан болса. Бұл күй, клиент құрылғысы Басқару серверімен синхрондалмайынша қала береді; синхрондалғаннан кейін анықтау тізімнен жоғалады.

  Растау – егер әкімші бұл анықтауды өңдеп, оны расталған болса. Бұл күй, клиент құрылғысы Басқару серверімен синхрондалмайынша қала береді; синхрондалғаннан кейін анықтау тізімнен жоғалады.

  Бос – егер әкімші бұл анықтауды өңдемеген болса.

- **Жалпы уақыт ережелері іске қосылды**

  Бір эвристикалық ережені, бір процесті және бір клиент құрылғысын анықтау саны. Бұл санды Kaspersky Endpoint Security есептеп шығарған.

- **Пайдаланушы аты**

  Анықтауды тудырған процесті іске қосқан клиент құрылғысының пайдаланушы аты.

- **Бастапқы өңдеу жолы**

  Бастапқы өңдеу жолы, яғни әрекетті орындаған процеске апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Бастапқы өңдеу хэші**

  Бастапқы процесс файлының SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Бастапқы нысан жолы**

  Процесті іске қосқан нысанға апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Бастапқы нысан хэші**

  Бастапқы файлдың SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты өңдеу жолы**

  Мақсатты процеске апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты өңдеу хэші**

  Мақсатты файлдың SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты нысан жолы**

  Мақсатты нысанға апаратын жол (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Мақсатты нысан хэші**

  Мақсатты файлдың SHA256 хэші (толық ақпаратты Kaspersky Endpoint Security анықтамасынан қараңыз).

- **Өңделді**

  Аномалияның анықталған күні.

Әрбір элементтің сипаттарын қарау үшін:

1. Консоль ағашында Басқару серверінің қажетті түйінін таңдаңыз.
2. **"Смарт оқыту" күйіндегі ереже триггерлері** ішкі қалтасын таңдаңыз (әдепкі бойынша ол **Кеңейтілген → Қоймалар** қалтасында орналасқан).
3. **"Смарт оқыту" күйіндегі ереже триггерлері** қалтасының жұмыс аймағында қажетті нысанды таңдаңыз.
4. Келесі әрекеттердің бірін орындаңыз:

   - Экранның оң жағындағы жұмыс аймағында **Сипаттар** сілтемесінен өтіңіз.
   - Нысанның контекстік мәзірінде **Сипаттар** тармағын таңдаңыз.

   Ашылған нысан сипаты терезесінде нысан туралы ақпарат көрсетіледі.

Сіз Аномалияларды бейімделумен басқару ережелері анықтаған тізімдегі кез келген нысанды растай аласыз немесе ерекшеліктерге қоса аласыз.

Нысанды растау үшін,

анықтау тізімінен бір немесе бірнеше элементті таңдап, **Растау** түймесін басыңыз.

Элементтер күйі **Расталуда** болып өзгереді.

Сіздің растауыңыз ережелер қолданатын статистикаға әсер етеді (толық ақпаратты Kaspersky Endpoint Security 11 for Windows анықтамасынан қараңыз).

Нысанды ерекшеліктерге қосу үшін,

Анықтау тізімі нысанының (немесе бірнеше нысанының) контекстік мәзірінде **Ерекшеліктерге қосу** тармағын таңдаңыз.

Нәтижесінде, ерекшелікті қосу шебері іске қосылады. Шебердің нұсқауларын орындаңыз.

Егер сіз нысанды қабылдамасаңыз немесе растасаңыз, ол клиент құрылғысы Басқару серверімен келесі рет синхрондалғаннан кейін анықтау тізімінен шығарылады және бұдан былай тізімде көрсетілмейді.

Аномалияларды бейімделумен басқару ережесіне ерекшеліктер қосу

Ерекшелікті қосу шебері Kaspersky Endpoint Security үшін Аномалияларды бейімделумен басқару ережелерінен ерекшеліктерді қосуға мүмкіндік береді.

Төмендегі тәсілдердің бірін пайдаланып, шеберді іске қосуға болады.

Аномалияларды бейімделумен басқару қалтасындағы ерекшелікті қосу шеберін іске қосу үшін:

1. Консоль ағашында өзіңізге қажетті Басқару серверінің атауы бар торапты таңдаңыз.

2. **"Смарт оқыту" күйіндегі ереже триггерлері** ішкі қалтасын таңдаңыз (әдепкі бойынша ол **Кеңейтілген → Қоймалар** қалтасында орналасқан).

3. Жұмыс аймағында нысанның (немесе бірнеше нысанның) контекстік мәзіріндегі анықтау тізімінен **Ерекшеліктерге қосу** тармағын таңдаңыз.

   Бір уақытта 1000-ға дейін ерекшелік қосуға болады. Егер сіз көбірек элементтерді таңдап, оларды ерекшеліктерге қосуға тырыссаңыз, қате туралы хабар пайда болады.

Нәтижесінде, ерекшелікті қосу шебері іске қосылады.

Консоль ағашындағы басқа түйіндерден ерекшелікті қосу шеберін іске қосу үшін:

- Басқару серверінің негізгі терезесінің **Оқиғалар** қойыншасын ашып, **Пайдаланушылардың сұраулары** немесе **Соңғы оқиғалар** тармағын таңдаңыз.

- **Аномалияларды бейімделумен басқару ережелерінің күйі туралы есеп** терезесінде **Анықтамалар саны** бағанын таңдаңыз.

1-қадам. Бағдарламаны лицензиялау

Егер сізде тек Kaspersky Endpoint Security for Windows бағдарламасы болса және Аномалияларды бейімделумен басқару ережелерін қолдайтын басқа бағдарламалар болмаса, бұл қадамды өткізіп жіберуге болады.

Ерекшелікті қосу шебері Kaspersky бағдарламаларының тізімін көрсетеді, олар үшін басқару плагиндері осы бағдарламаларға арналған саясаттарға ерекшеліктер қосуға мүмкіндік береді. Тізімнен бағдарламаны таңдап, ерекшелік қосылатын саясатты таңдауды жалғастыру үшін **Келесі** түймесін басыңыз.

2-қадам. Саясатты (саясаттарды) таңдау

Шебер Kaspersky Endpoint Security үшін саясаттар тізімін (саясат профильдерімен) көрсетеді.

Ерекшеліктер қосқыңыз келетін барлық саясаттар мен саясат профильдерін таңдап, **Келесі** түймесін басыңыз.

3-қадам. Саясатты (саясаттарды) өңдеу

Шебер саясатты өңдеу барысын көрсетеді. **Бас тарту** түймесін басып, саясатты өңдеуді доғаруға болады.

Иеленген саясаттарды жаңарту мүмкін емес. Саясатты өзгертуге құқықтарыңыз болмаса, мұндай саясат та жаңартылмайды.

Барлық саясаттар өңделгеннен (немесе саясаттарды өңдеу доғарылғаннан) кейін, есеп жасалады. Есеп, қандай саясаттардың сәтті жаңартылғанын (жасыл белгіше), қандай саясаттардың жаңартылмағанын (қызыл белгіше) көрсетеді.

Бұл қадамның соңғы қадамы. Шебердің жұмысын аяқтау үшін **Дайын** түймесін басыңыз.

Карантин және сақтық көшірмелеу

Клиент құрылғыларында орнатылған Kaspersky антивирустық бағдарламалары, құрылғыларды сканерлеу процесінде файлдарды карантинге немесе резервтік сақтау орнына орналастыра алады.

Карантин – анықтау сәтінде ықтимал вирус жұққан немесе емдеу мүмкін емес файлдар орналастырылатын арнайы қойма.

Сақтық көшірмелеу емдеу барысында жойылған немесе өзгертілген файлдардың сақтық көшірмелерін сақтауға арналған.

Kaspersky Security Center, құрылғылардағы Kaspersky бағдарламалары карантинге және резервтік сақтау орнына орналастырған файлдардың жалпы тізімін құрастырады. Клиент құрылғыларының Желілік агенттері карантиндегі және резервтік сақтау орындарындағы файлдар туралы ақпаратты Басқару серверіне жібереді. Басқару консолі арқылы құрылғылардағы сақтау орындарындағы файлдардың сипаттарын қарап шығуға, сақтау орындарының зиянды БЖ-ын тексеруді іске қосуға және олардан файлдарды жоюға болады. Файлдар күйінің белгішелері қолданбада сипатталған.

Карантин және сақтық көшірме операцияларында Kaspersky Endpoint Security-ге қолдау көрсетіледі.

Kaspersky Security Center файлдарды сақтау орындарынан Басқару серверіне көшірмейді. Барлық файлдар құрылғылардағы сақтау орындарында орналастырылады. Файлдарды қалпына келтіру, файлды сақтау орнына қойылған қауіпсіздік бағдарламасы орнатылған құрылғыда жүзеге асырылады.

Сақтау орындарындағы файлдарды қашықтан басқаруды қосу

Әдепкі бойынша, клиент құрылғыларындағы қоймалардағы файлдарды қашықтан басқару өшірілген.

Клиент құрылғыларындағы қоймалардағы файлдарды қашықтан басқаруды қосу үшін:

1. Консоль ағашында қойма файлдарын қашықтан басқаруды қосуды қажет ететін басқару тобын таңдаңыз.
2. Топтың жұмыс аймағында **Саясаттар** қойыншасын ашыңыз.
3. **Саясаттар** қойыншасында файлдарды құрылғылардағы қоймаларға орналастыратын қауіпсіздік бағдарламасының саясатын таңдаңыз.
4. **Басқару серверін хабарландыру** блогындағы саясат сипаттары терезесінде, қашықтан басқаруды қосқыңыз келетін қоймаларға сай келетін жалаушаларды қойыңыз.

   Басқару серверін хабарландыру блогының саясат сипаттары терезесінде орналасуы және блоктағы жалаушалардың атауы әрбір қауіпсіздік бағдарламасы үшін бірегей.

Сақтау орнына қойылған файлдың сипаттарын қарап шығу

Карантинге немесе резервтік сақтау орнына қойылған файлдың сипаттарын қарап шығу үшін:

1. **Қоймалар** қалтасындағы Консоль ағашында салынған **Карантин** немесе **Сақтық көшірмелеу** қалтасын таңдаңыз.

2. **Карантин** (**Сақтық көшірмелеу**) қалтасының жұмыс аймағында, параметрлерін қарап шығу қажет болған файлды таңдаңыз.

3. Файлдың мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

Сақтау орнындағы файлдарды жою

Карантинге немесе резервтік сақтау орнына орналастырылған файлды жою үшін:

1. **Қоймалар** қалтасындағы Консоль ағашында салынған **Карантин** немесе **Сақтық көшірмелеу** қалтасын таңдаңыз.

2. **Карантин** (немесе **Сақтық көшірмелеу**) қалтасының жұмыс аймағында **Shift** және **Ctrl** пернелерін қолдана отырып, жою қажет болған файлдарды таңдаңыз.

3. Файлдарды келесі тәсілдердің бірімен жойыңыз:

   - Файлдың мәнмәтіндік мәзірінде **Жою** тармағын таңдаңыз.

   - Таңдалған файлдары бар жұмыс блогында бір файлды жою кезінде **Жою** (**Жою**) сілтемесі бойынша.

Нәтижесінде, таңдалған файлдарды клиент құрылғыларындағы сақтау орындарына орналастырған қауіпсіздік бағдарламалары файлдарды осы сақтау орындарынан жояды.

Сақтау орнындағы файлдарды қалпына келтіру

Карантинге немесе резервтік сақтау орнына орналастырылған файлды қалпына келтіру үшін:

1. **Қоймалар** қалтасындағы Консоль ағашында салынған **Карантин** немесе **Сақтық көшірмелеу** қалтасын таңдаңыз.

2. **Карантин** (**Сақтық көшірмелеу**) қалтасының жұмыс аймағында **Shift** және **Ctrl** пернелерін қолдана отырып, қалпына келтіру қажет болған файлдарды таңдаңыз.

3. Файлдарды қалпына келтіру процесін келесі тәсілдердің бірімен іске қосыңыз:

   - Файлдың мәнмәтіндік мәзірінде **Қалпына келтіру** тармағын таңдаңыз.

   - Таңдалған файлдармен жұмыс блогында **Қалпына келтіру** сілтемесі бойынша.

Нәтижесінде, клиент құрылғыларындағы сақтау орындарына файлдарды орналастырған қауіпсіздік бағдарламалары осы файлдарды бастапқы қалталарға қалпына келтіреді.

Сақтау орнындағы файлды дискіге сақтау

Kaspersky Security Center, қауіпсіздік бағдарламасы карантинге немесе клиент құрылғысындағы резервтік сақтау орнына орналастырған файлдардың көшірмелерін дискіге сақтауға мүмкіндік береді. Файлдар Kaspersky Security Center орнатылған құрылғыға, сіз көрсеткен қалтаға көшіріледі.

Файлдың көшірмесін карантиннен немесе резервтік сақтау орнынан қатты дискіге сақтау үшін:

1. **Қоймалар** қалтасындағы Консоль ағашында салынған **Карантин** немесе **Сақтық көшірмелеу** қалтасын таңдаңыз.

2. **Карантин** (**Сақтық көшірмелеу**) қалтасының жұмыс аймағында қатты дискіге көшіру қажет болған файлды таңдаңыз.

3. Файлды көшіру процесін келесі тәсілдердің бірімен іске қосыңыз:

   - Файлдың мәнмәтіндік мәзірінде **Дискіге сақтау** тармағын таңдаңыз.

   - Таңдалған файлмен жұмыс блогында **Дискіге сақтау** сілтемесін басыңыз.

Нәтижесінде, клиент құрылғысында файлды карантинге орналастырған қауіпсіздік бағдарламасы файлдың көшірмесін көрсетілген қалтаға сақтайды.

Карантиндегі файлдарды сканерлеу

Карантиндегі файлдарды тексеру үшін:

1. **Қоймалар** қалтасындағы консоль шежіресінен **Карантин** салынған қалтасын таңдаңыз.

2. **Карантин** қалтасының жұмыс аймағында **SHIFT** және **CTRL** пернелерінің көмегімен тексеру қажет болған файлдарды таңдаңыз.

3. Файлдарды тексеру процесін келесі тәсілдердің бірімен іске қосыңыз:

   - Файлдың контекстік мәзірінде **Тексеру** тармағын таңдаңыз.

   - Таңдалған файлдармен жұмыс блогында **Тексеру** сілтемесі бойынша.

Қолданба таңдалған файлдарды карантинге қойған қауіпсіздік қолданбалары үшін осы файлдар сақталатын құрылғыларда талап ету бойынша сканерлеу тапсырмасын іске қосады.

Белсенді қауіптер

Клиент құрылғыларында табылған кейін өңделетін файлдар туралы ақпарат **Қоймалар** қалтасында, **Белсенді қауіптер** ішкі қалтасында болады.

Кейінге қалдырылған өңдеу мен дезинфекцияны қауіпсіздік бағдарламасы сұрау бойынша немесе белгілі бір оқиғадан кейін орындайды. Файлдарды кешіктіріп зарарсыздандыру файлдарының параметрлерін конфигурациялауға болады.

Кейін өңделетін файлды дезинфекциялау

Кейін өңделетін файлды зарарсыздандыруды іске қосу үшін:

1. **Қоймалар** қалтасындағы консоль шежіресінен **Белсенді қауіптер** салынған қалтасын таңдаңыз.
2. **Белсенді қауіптер** қалтасының жұмыс аймағында зарарсыздандыру қажет болған файлды таңдаңыз.
3. Файлды зарарсыздандыру процесін келесі тәсілдердің бірімен іске қосыңыз:
   - Файлдың мәнмәтіндік мәзірінде **Зарарсыздандыру** тармағын таңдаңыз.
   - Таңдалған файлымен жұмыс істеу блогындағы **Зарарсыздандыру** сілтемесі бойынша.

   Нәтижесінде, файлды зарарсыздандыру әрекеті орындалады.

Файл зарарсыздандырылған болса, клиент құрылғысына орнатылған қауіпсіздік бағдарламасы оны бастапқы қалтаға қалпына келтіреді. Файл туралы жазба **Белсенді қауіптер** қалтасындағы тізімнен жойылады. Файлды зарарсыздандыру мүмкін болмаса, құрылғыда орнатылған қауіпсіздік бағдарламасы файлды құрылғыдан жояды. Файл туралы жазба **Белсенді қауіптер** қалтасындағы тізімнен жойылады.

> Орнатылған қауіпсіздік бағдарламасына, оның нұсқасы мен параметрлеріне байланысты файлдарды зарарсыздандыру мен жою мүмкіндіктері әртүрлі болуы мүмкін.

Кейін өңделетін файлды дискіге сақтау

Kaspersky Security Center, клиент құрылғыларында анықталған кейін өңделетін файлдардың көшірмелерін дискіге сақтауға мүмкіндік береді. Бұл қолданба өңдеген немесе жойған файлдарға қатысты. Файлдар Kaspersky Security Center орнатылған құрылғыға, сіз көрсеткен қалтаға көшіріледі.

Залалсыздандыру кезінде жойылған немесе өзгертілген файлдардың көшірмелерін файлдар жадта сақталған болса сақтай аласыз. Басқарылатын құрылғыдағы Windows жүйесіне арналған Kaspersky Endpoint Security.

Кейін өңделетін файлдың көшірмесін дискіге сақтау үшін:

1. **Қоймалар** қалтасындағы консоль шежіресінен **Белсенді қауіптер** салынған қалтасын таңдаңыз.
2. **Белсенді қауіптер** қалтасының жұмыс аймағында дискіге көшіру қажет болған файлдарды таңдаңыз.
3. Файлды көшіру процесін келесі тәсілдердің бірімен іске қосыңыз:
   - Файлдың мәнмәтіндік мәзірінде **Дискіге сақтау** тармағын таңдаңыз.
   - Таңдалған файлмен жұмыс блогында **Дискіге сақтау** сілтемесін басыңыз.

Нәтижесінде, таңдалған кейін өңделетін файл анықталған клиент құрылғысының қауіпсіздік бағдарламасы файлдың көшірмесін көрсетілген қалтаға сақтайды.

"Белсенді қауіптер" қалтасындағы файлдарды жою

***Белсенді қауіптер** қалтасындағы файлды жою үшін:*

1. **Қоймалар** қалтасындағы консоль шежіресінен **Белсенді қауіптер** салынған қалтасын таңдаңыз.
2. **Белсенді қауіптер** қалтасының жұмыс аймағында **SHIFT** және **CTRL** пернелерінің көмегімен жою қажет болған файлдарды таңдаңыз.
3. Файлдарды келесі тәсілдердің бірімен жойыңыз:
   - Файлдың мәнмәтіндік мәзірінде **Жою** тармағын таңдаңыз.
   - Таңдалған файлдары бар жұмыс блогында бір файлды жою кезінде **Жою** (**Жою**) сілтемесі бойынша.

Нәтижесінде, таңдалған файлдарды клиент құрылғыларындағы сақтау орындарына орналастырған қауіпсіздік бағдарламалары файлдарды осы сақтау орындарынан жояды. Файлдар туралы жазбалар **Белсенді қауіптер** қалтасындағы тізімнен жойылады.

Kaspersky Security Network (KSN)

Бұл бөлімде Kaspersky Security Network (KSN) онлайн-қызметтері инфрақұрылымын қолдану тәсілі сипатталған. KSN туралы ақпарат, сондай-ақ KSN қосу, KSN бағдарламасына қатынасуды конфигурациялау, KSN прокси-серверін пайдалану статистикасын қарау бойынша нұсқаулар берілген.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

KSN туралы

Kaspersky Security Network (KSN) – файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы Kaspersky жедел білім базасына қатынасуды ұсынатын онлайн-қызметтер инфрақұрылымы. Kaspersky Security Network деректерін пайдалану Kaspersky бағдарламаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады. KSN қолданбасы Kaspersky беделдік дерекқорларынан басқарылатын құрылғыларға орнатылған қолданбалар туралы ақпаратты алуға мүмкіндік береді.

Kaspersky Security Center қолданбасы келесі инфрақұрылымдық шешімдерін қолдайды:

- *KSN* – Kaspersky Security Network қолданбасымен ақпарат алмасуға мүмкіндік беретін шешім. KSN бағдарламасына қатыса отырып, сіз автоматты режимде Kaspersky ұйымына Kaspersky Security Center басқаратын клиент құрылғыларына орнатылған Kaspersky бағдарламаларының жұмысы туралы ақпарат беруге келісесіз. Ақпаратты беру, конфигурацияланған KSN бағдарламасына қатынасу параметрлеріне сәйкес орындалады. Kaspersky мамандары алынған ақпаратты қосымша талдап, оны Kaspersky Security Network беделдік және статистикалық дерекқорларына қосады. Kaspersky Security Center бағдарламасы осы шешімді әдепкі бойынша қолданады.

- *Kaspersky Private Security Network (KPSN)* – бұл Kaspersky қолданбалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан жаһандық KSN қолданбасына деректерді жібермей, Kaspersky Security Network дерекқорларына және басқа да статистикалық деректерге қол жеткізуді қамтамасыз ететін шешім. KPSN келесі себептердің бірі бойынша Kaspersky Security Network бағдарламасына қатыса алмайтын ұйымдарға арналған:

  - Пайдаланушы құрылғылары интернетке қосылмаған.

  - Кез келген деректерді елден немесе корпоративтік желіден (LAN) тыс жерге жіберуге заңмен немесе корпоративті қауіпсіздік саясаттарымен тыйым салынады.

  Басқару сервері терезесінің **KSN-прокси параметрлері** бөлімінде Kaspersky Private Security Network қатынасу параметрлерін конфигурациялай аласыз.

Бағдарлама, бағдарламаны жылдам іске қосу шеберінің жұмысы барысында KSN бағдарламасына қосылуға ұсынады. Қолданбаны пайдаланған кезде, KSN-ді пайдалануды кез келген уақытта бастауға не тоқтатуға болады.

Сіз KSN бағдарламасын KSN қосу кезінде оқитын және қабылдайтын KSN мәлімдемесіне сай қолданасыз. KSN мәлімдемесі жаңартылған болса, ол басқару серверін алдыңғы нұсқасынан жаңарту кезінде көрсетіледі. Сіз жаңартылған KSN мәлімдемесін қабылдауға немесе қабылдамауға болады. Оны қабылдамасаңыз, сіз бұған дейін қабылдаған KSN мәлімдемесінің алдыңғы нұсқасына сәйкес KSN бағдарламасын қолдануды жалғастырасыз.

KSN қосулы болған кезде, Kaspersky Security Center бағдарламасы KSN серверлерінің қолжетімді болуын тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Бұл, қауіпсіздік деңгейіне басқарылатын құрылғылар үшін қолдау көрсетілетіндігіне көз жеткізу үшін керек.

Басқару сервері басқаратын клиент құрылғылары KSN бағдарламасымен KSN прокси-серверінің көмегімен өзара әрекеттеседі. KSN прокси-сервері қызметі келесі мүмкіндіктерді ұсынады:

- Клиент құрылғылары, тіпті интернетке тікелей қатынасу мүмкіндігі болмаса да, KSN бағдарламасына сұраулар жасай алады, KSN бағдарламасынан ақпарат ала алады және KSN бағдарламасына ақпаратты жібере алады.

- KSN прокси-сервері өңделген деректерді кэштей отырып сыртқы желіге арнаға түсетін жүктемені азайтады және клиент құрылғысының сұралған ақпаратты алуын тездетеді.

Сіз KSN прокси-сервері параметрлерін Басқару сервері сипаттары терезесінің **KSN-прокси параметрлері** бөлімінде конфигурациялай аласыз.

Kaspersky Security Network бағдарламасына қатынасуды конфигурациялау

Kaspersky Security Network (KSN) бағдарламасына Басқару серверінен және тарату нүктесінен қатынасуды белгілеуге болады.

Басқару серверінің Kaspersky Security Network (KSN) желісіне қатынасуын конфигурациялау үшін:

1. Консоль ағашында KSN бағдарламасына қатынасуды конфигурациялау үшін Басқару серверін таңдаңыз.

2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.

3. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **KSN Проксиі** → **KSN-прокси параметрлері** бөлімін таңдаңыз.

4. KSN прокси-сервері қызметін пайдалану үшін **Басқару серверін прокси-сервер ретінде пайдалану** жалаушасын қойыңыз.

   KSN-де клиент құрылғыларынан деректерді беру клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security саясатымен реттеледі. Егер жалауша алынып тасталса, KSN бағдарламасына Басқару серверінен және клиент құрылғыларынан Kaspersky Security Center арқылы деректерді берілмейді. Бұл ретте, клиент құрылғылары өздерінің параметрлеріне сәйкес деректерді KSN бағдарламасына тікелей (Kaspersky Security Center арқылы емес) жібере алады. Клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security for Windows саясаты осы құрылғылардың қандай деректерін тікелей (Kaspersky Security Center арқылы емес) KSN бағдарламасына жіберетінін анықтайды.

5. **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрін қосыңыз.

   Егер параметр қосулы болса, клиент құрылғылары патчтарды орнату нәтижелерін Kaspersky бағдарламасына жібереді. Бұл параметрді қосқан кезде KSN мәлімдемесі шарттарын оқып, қабылдағаныңызға көз жеткізіңіз.

   Kaspersky Private Security Network қолдансаңыз, KPSN (pkcs7 және pem кеңейтімдері бар файлдар) параметрлерін жүктеп алу үшін **KPSN конфигурациялау** опциясын қосып, **KSN-прокси парам. бар файлды таңдау** түймесін басыңыз. Параметрлер жүктелгеннен кейін, интерфейсте провайдердің атауы, провайдердің контактілері және KPSN параметрлері бар файл жасалған күн көрсетіледі.

   > KSN қосылған кезде, KSN сұрауларын тікелей KSN бұлтты қызметіне жіберуге конфигурацияланған тарату нүктелеріне назар аударыңыз. Желілік агенттің 11 (немесе одан бұрынғы) нұсқасы орнатылған тарату нүктелері KSN бұлтты қызметіне тікелей қатынаса алмайды. KSN сұрауларын KPSN-ге жіберу үшін тарату нүктелерін қайта реттеу мақсатында әр тарату нүктесіне **KSN сұрауын Басқару серверіне қайта жіберу** параметрін қосыңыз. Бұл параметрді тарату нүктесінің немесе Желілік агент саясатының сипаттарында қосуға болады.

   KPSN конфигурациялау жалаушасын қойғанда, KPSN туралы ақпараты бар хабар пайда болады.

   Kaspersky Security Center жүйесінде **KPSN конфигурациялау** опциясын қоссаңыз, бұл қолданбалар қолдау көрсетілетін KPSN туралы ақпарат алады. Қолданба сипаттары терезесіндегі **Кеңейтілген қорғаныс** бөлімінің **Kaspersky Security Network** бөлімшесінде KSN: KSN немесе KPSN жеткізушісі көрсетіледі.

KPSN қолданбасымен жұмыс істеу үшін Kaspersky Security for Virtualization 3.0, агентсіз қорғаныс Service Pack 2 нұсқасынан төмен немесе Kaspersky Security for Virtualization 3.0 Service Pack 1, жеңіл агент нұсқасынан төмен қолданбаларды пайдалансаңыз, KPSN қолданбасын пайдалану конфигурацияланбаған қосалқы басқару серверлерін пайдалану ұсынылады.

KSN Проксиі → **KSN-прокси параметрлері** бөліміндегі басқару сервері сипаттары терезесінде KSN орнатылған болса, Kaspersky Security Center жүйесі Kaspersky Security Network статистикасын жібермейді.

Прокси-сервер параметрлері басқару сервері сипаттарында орнатылса, бірақ желі архитектурасы KPSN-ді тікелей пайдалануды талап ететін болса, **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу** жалаушасын қойыңыз. Әйтпесе, басқарылатын қолданбадан сұрау KPSN қолданбасына берілмейді.

6. Басқару серверін KSN прокси-сервері қызметіне қосу параметрлерін конфигурациялаңыз:

   - **Қосылым параметрлері** блогында, **TCP порты** енгізу өрісінде, KSN прокси-серверіне қосылу орындалатын TCP порты нөмірін көрсетіңіз. Әдепкі бойынша, KSN прокси-серверіне қосылу 13111-порт арқылы жүзеге асырылады.

   - Басқару серверін UDP порты арқылы KSN прокси-серверіне қосу үшін **UDP портын пайдалану** параметрін таңдап, **UDP порты** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі, TCP порты қолданылады. Егер параметр қосулы болса, әдепкі бойынша KSN прокси-серверіне қосылу 15111 санды UDP порты арқылы жүзеге асырылады.

   - Басқару серверін HTTPS порты арқылы KSN прокси-серверіне қосу үшін **HTTPS порт арқылы пайдаланыңыз** опциясын қосып, порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі, TCP порты қолданылады. Егер параметр қосулы болса, әдепкі бойынша KSN прокси-серверіне қосылу 17111 санды HTTPS порты арқылы жүзеге асырылады.

7. **Қосалқы Басқару серверлерін KSN желісіне негізгі Басқару сервері арқылы қосу** параметрін қосыңыз.

   Егер бұл параметр қосулы болса, кез келген иерархия деңгейіндегі қосалқы Басқару серверлері негізгі Басқару серверін KSN прокси-сервері ретінде пайдаланады. Егер бұл параметр өшірулі болса, қосалқы Басқару серверлері KSN бағдарламасына өздігінен қосылады. Бұл жағдайда, басқарылатын құрылғылар қосалқы Басқару серверлерін KSN прокси-серверлері ретінде пайдаланады.

   Егер **KSN-прокси параметрлері** бөліміндегі қосалқы Басқару серверлерінің сипаттарында да **Басқару серверін прокси-сервер ретінде пайдалану** жалаушасы қойылса, қосалқы Басқару серверлері негізгі Басқару серверін прокси-сервер ретінде пайдаланады.

8. **OK** түймесін басыңыз.

Нәтижесінде, KSN бағдарламасына қатынасу параметрлері сақталады.

Сондай-ақ, KSN бағдарламасына тарату нүктесі жағынан қатынасуды конфигурациялауға болады, мысалы, Басқару серверіне жүктемені азайту қажет болса. KSN прокси-серверінің рөлін атқаратын тарату нүктесі, Басқару серверін айналып өтіп, басқарылатын құрылғылардан келетін KSN сұрауларын тікелей Kaspersky бағдарламасына жібереді.

Тарату нүктесінің Kaspersky Security Network (KSN) бағдарламасына қатынасуын конфигурациялау үшін:

1. Тарату нүктесі қолмен тағайындалғанына көз жеткізіңіз.
2. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
3. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
4. Басқару сервері сипаттары терезесінде **Тарату нүктелері** бөлімін таңдаңыз.
5. Тізімнен тарату нүктесін таңдап, **Сипаттар** түймесі арқылы оның сипаттары терезесін ашыңыз.
6. Тарату нүктесінің сипаттары терезесінде **KSN прокси сервері** бөлімінде **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру** таңдаңыз.
7. **ОК** түймесін басыңыз.

Тарату нүктесі KSN прокси-серверінің рөлін атқарады.

KSN қосу және өшіру

KSN қосу үшін:

1. Консоль ағашында KSN қосу қажет Басқару серверін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде, **KSN Проксиі** бөлімінде **KSN-прокси параметрлері** бөлікшесін таңдаңыз.
4. **Басқару серверін прокси-сервер ретінде пайдалану** таңдаңыз.

   Нәтижесінде, KSN прокси-сервері қызметі қосылады.
5. **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** жалаушасын қойыңыз.

   Нәтижесінде, KSN қосулы болады.

   Жалауша орнатылған болса, клиент құрылғылары патчтарды орнату нәтижелерін Kaspersky бағдарламасына жібереді. Жалаушаны қоя отырып, сіз KSN мәлімдемесін оқып шығып, қабылдауыңыз керек.
6. **ОК** түймесін басыңыз.

KSN өшіру үшін:

1. Консоль ағашында KSN қосу қажет Басқару серверін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде, **KSN Проксиі** бөлімінде **KSN-прокси параметрлері** бөлікшесін таңдаңыз.
4. KSN прокси-сервері қызметін өшіру үшін **Басқару серверін прокси-сервер ретінде пайдалану** жалаушасын алып тастаңыз немесе **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** жалаушасын алып тастаңыз.

Жалауша алынып тасталған болса, клиент құрылғылары патчтарды орнату нәтижелерін Kaspersky бағдарламасына жібермейді.

KSN қолдансаңыз, **KPSN конфигурациялау** жалаушасын алып тастаңыз.

Нәтижесінде, KSN өшірулі болады.

5. **OK** түймесін басыңыз.

Қабылданған KSN мәлімдемесін қарау

Kaspersky Security Network (KSN) қосқан кезде сіз KSN мәлімдемесін оқып, қабылдауыңыз керек. Сіз қабылданған KSN мәлімдемесін кез келген уақытта көре аласыз.

Қабылданған KSN мәлімдемесін қарап шығу үшін:

1. Консоль ағашында KSN қосылған Басқару серверін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде, **KSN Проксиі** бөлімінде **KSN-прокси параметрлері** бөлікшесін таңдаңыз.
4. **Қабылданған KSN мәлімдемесін қарау** сілтемесінен өтіңіз.

Ашылған терезеде сіз қабылданған KSN мәлімдемесінің мәтінін көре аласыз.

KSN прокси-сервері статистикасын қарау

KSN прокси-сервері – бұл Kaspersky Security Network инфрақұрылымы мен Басқару сервері басқаратын клиент құрылғылары арасындағы өзара іс-қимылды қамтамасыз ететін қызмет.

KSN прокси-серверін қолдану сізге келесі мүмкіндіктерді ұсынады:

- Клиент құрылғылары, тіпті интернетке тікелей қатынасу мүмкіндігі болмаса да, KSN бағдарламасына сұраулар жасай алады және KSN бағдарламасына ақпаратты жібере алады.
- KSN прокси-сервері өңделген деректерді кэштей отырып сыртқы желіге арнаға түсетін жүктемені азайтады және клиент құрылғысының сұралған ақпаратты алуын тездетеді.

Басқару сервері сипаттары терезесінде сіз KSN прокси-сервері параметрлерін конфигурациялай аласыз және KSN прокси-серверін пайдалану туралы статистикалық ақпаратты көре аласыз.

KSN прокси-сервері жұмысының статистикасын қарау үшін:

1. Консоль ағашында KSN статистикасын қарау қажет Басқару серверін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. Басқару сервері сипаттары терезесінде, **KSN Проксиі** бөлімінде **KSN Проксиі статистикасы** бөлікшесін таңдаңыз.

   Бұл бөлімде KSN прокси-сервері жұмысының нақты статистикасы (кэштегі жазбалар саны, кэштегі өңделген пакеттер және қабылданған пакеттер саны) көрсетіледі. Сондай-ақ, Басқару сервері KSN желісіне қосылған болса, сәйкес ақпараттық хабарлар көрсетіледі.

Қажет болса, қосымша әрекеттерді орындаңыз:

- **Жаңарту** түймесі арқылы KSN прокси-серверін қолдану туралы статистикалық ақпаратты жаңартыңыз;
- **Файлға экспортталуда** түймесі арқылы статистика деректерін CSV пішіміндегі файлға экспорттаңыз;
- **KSN қосылымын тексеру** түймесі арқылы Басқару сервері қазіргі сәтте KSN бағдарламасына қосылғанын тексеріңіз.

4. Басқару сервері сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

Жаңартылған KSN мәлімдемесін қабылдау

Сіз KSN бағдарламасын KSN қосу кезінде оқитын және қабылдайтын KSN мәлімдемесіне сай қолданасыз. KSN мәлімдемесі жаңартылған болса, ол Басқару серверін жаңарту кезінде немесе Басқару серверін алдыңғы нұсқасынан жаңарту кезінде көрсетіледі. Сіз жаңартылған KSN мәлімдемесін қабылдауға немесе қабылдамауға болады. Оны қабылдамасаңыз, сіз бұған дейін қабылдаған KSN мәлімдемесінің нұсқасына сәйкес KSN бағдарламасын қолдануды жалғастырасыз.

Басқару серверін жаңартқаннан немесе Басқару серверін алдыңғы нұсқасынан жаңартқаннан кейін, жаңартылған KSN мәлімдемесі автоматты түрде көрсетіледі. Жаңартылған KSN мәлімдемесін қабылдамасаңыз, оны бәрібір кейінірек қарап шыға аласыз және қабылдай аласыз.

Жаңартылған KSN мәлімдемесін қарап шығу және қабылдау немесе қабылдамау үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. **Мониторинг** қойыншасында, **Мониторинг** бөлімінде **Қабылданған Kaspersky Security Network мәлімдемесі ескірген** сілтемесінен өтіңіз.

   KSN мәлімдемесі терезесі ашылады.
3. KSN мәлімдемесін мұқият оқып шығыңыз, содан соң шешім қабылдаңыз. Жаңартылған KSN мәлімдемесінің шарттарын қабылдасаңыз, **Лицензиялық келісімнің шарттарын қабылдаймын** түймесін басыңыз. Жаңартылған KSN мәлімдемесінің шарттарын қабылдамасаңыз, **Бас тарту** түймесін басыңыз.

Сіздің таңдауыңызға байланысты KSN ағымдағы немесе жаңартылған KSN мәлімдемесінің шарттарына сәйкес жұмысын жалғастырады. Сіз кез келген уақытта қабылданған KSN мәлімдемесі мәтінін Басқару сервері сипаттарынан көре аласыз.

Kaspersky Security Network көмегімен қосымша қорғау

Kaspersky ұйымы Kaspersky Security Network көмегімен қосымша қорғау деңгейін ұсынады. Осы қорғаныс тәсілі, күрделілігі жоғары тұрақты қауіптер мен нөлдік күндік қауіптеріне қарсы тиімді күресуге бағытталған. Kaspersky Endpoint Security бағдарламасымен біріктірілген бұлтты технологиялар және Kaspersky вирус талдаушыларының сараптамалық білімі желідегі ең күрделі қауіптерге қарсы күшті қорғаныста қамтамасыз етеді.

Kaspersky Endpoint Security бағдарламасындағы қосымша қорғау туралы қосымша ақпаратты Kaspersky веб-сайтынан таба аласыз.

Тарату нүктесі KSN прокси-сервері ретінде жұмыс істейтінін тексеру

Тарату нүктесі рөлін атқаратын басқарылатын құрылғыда KSN прокси-серверін қосуға болады. Басқарылатын құрылғыда ksnproxy қызметі іске қосылған болса, ол KSN прокси-сервері ретінде жұмыс істейді. Бұл қызметті құрылғыда жергілікті түрде қосуға немесе өшіруге болады.

Windows немесе Linux операциялық жүйесі бар құрылғыны тарату нүктесі ретінде тағайындауға болады. Тарату нүктесі қалай тексерілетіні осы тарату нүктесінің операциялық жүйесіне байланысты.

Тарату нүктесі Windows операциялық жүйесімен KSN прокси-сервері ретінде жұмыс істейтінін тексеру үшін:

1. Тарату нүктесі рөлін атқаратын құрылғыда Windows операциялық жүйесінде **Қызметтер** терезесін ашыңыз (**Барлық бағдарламалар** → **Басқару** → **Қызметтер**).

2. Қызметтер тізімінде KSN – ksnproxy прокси-сервері қызметі жұмыс істеп тұрғанын тексеріңіз.

   Егер ksnproxy қызметі жұмыс істеп тұрса, онда құрылғыдағы Желілік агент Kaspersky Security Network бағдарламасына қатысады және тарату нүктесінің әрекет ету ауқымына кіретін басқарылатын құрылғылар үшін KSN Proxy прокси-сервері ретінде жұмыс істейді.

Қажет болса, ksnproxy қызметін өшіруге болады. Бұл жағдайда, тарату нүктесінде Желілік агент бұдан былай Kaspersky Security Network бағдарламасына қатыспайды. Бұл үшін, жергілікті әкімші құқықтары керек.

Тарату нүктесі Linux операциялық жүйесімен KSN прокси-сервері ретінде жұмыс істейтінін тексеру үшін:

1. Тарату нүктесі ретінде әрекет ететін құрылғыда іске қосылған процестердің тізімі көрсетіледі.

2. Іске қосылған процестер тізімінде `/opt/kaspersky/ksc64/sbin/ksnproxy` процесінің іске қосылғанын тексеріңіз.

Егер `/opt/kaspersky/ksc64/sbin/ksnproxy` процесі іске қосылып тұрса, онда құрылғыдағы Желілік агент Kaspersky Security Network бағдарламасына қатысады және тарату нүктесінің әрекет ету ауқымына кіретін басқарылатын құрылғылар үшін KSN прокси-сервері ретінде жұмыс істейді.

Онлайн-анықтама мен офлайн анықтама арасында ауысу

Егер сізде интернетке қатынасу мүмкіндігі болмаса, сіз офлайн-анықтаманы пайдалана аласыз.

Онлайн-анықтама мен офлайн анықтама арасында ауысу үшін:

1. Kaspersky Security Center бағдарламасының басты терезесінде, консоль ағашында **Kaspersky Security Center 15.1** түйінін таңдаңыз.

2. **Глобалдық интерфейс параметрлері** сілтемесінен өтіңіз.

   Параметрлер терезесі ашылады.

3. Сипаттар терезесінде **Офлайн анықтаманы пайдалану** сілтемесін басыңыз.

4. **OK** түймесін басыңыз.

Параметрлер қолданылған және сақталған. Сіз кез келген уақытта параметрлерді өзгерте аласыз және кез келген уақытта онлайн-анықтаманы пайдалана бастай аласыз.

Оқиғаларды SIEM жүйелеріне экспорттау

Бұл бөлімде Kaspersky Security Center-де тіркелген оқиғаларды ақпараттық қауіпсіздік оқиғаларын басқару сыртқы жүйелеріне (SIEM жүйелері, Security Information and Event Management) экспорттау рәсімі сипатталған.

Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау

Kaspersky Security Center бағдарламасы конфигурациялауды бір тәсілмен орындауға мүмкіндік береді: Syslog пішімін пайдаланатын кез келген SIEM жүйесіне экспорттау, LEEF және CEF пішімдерін пайдаланатын QRadar, Splunk, ArcSight SIEM жүйелеріне экспорттау немесе оқиғаларды тікелей Kaspersky Security Center дерекқорынан SIEM жүйелеріне экспорттау. Осы сценарий аяқталғаннан кейін, Басқару сервері оқиғаларды автоматты түрде SIEM жүйесіне жібереді.

Алдын ала талаптар

Kaspersky Security Center бағдарламасына оқиғаларды экспорттауды конфигурациялауды бастамас бұрын:

- Оқиғаларды экспорттау әдістері туралы көбірек біліңіз.
- Сізде жүйелік параметрлердің мәндері бар екеніне көз жеткізіңіз.

> Сіз осы сценарийдің қадамдарын қалаған тәртіппен орындай аласыз.

Оқиғаларды SIEM жүйесіне экспорттау процесі келесі қадамдардан тұрады:

- **Kaspersky Security Center-ден оқиғаларды алу үшін SIEM жүйесін конфигурациялау**

  Нұсқаулар: Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау.

- **SIEM жүйесіне экспорттағыңыз келетін оқиғаны таңдау:**

  Нұсқаулар:

  - Басқару консолі: Syslog пішімінде экспорттау үшін Kaspersky бағдарламаларының оқиғаларын таңдау, Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау.
  - Kaspersky Security Center Web Console: Syslog пішімінде экспорттау үшін Kaspersky бағдарламаларының оқиғаларын таңдау, Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау.

- **Оқиғаларды SIEM жүйесіне экспорттауды келесі тәсілдердің бірімен конфигурациялау:**
  - TCP, UDP немесе TLS over TCP протоколдарын көрсетіңіз.

    Нұсқаулар:

    - Басқару консолі: Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау.
    - Kaspersky Security Center Web Console: Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау.
  - Оқиғаларды тікелей Kaspersky Security Center дерекқорынан экспорттауды пайдалану (жалпыға ортақ көріністер жиынтығы Kaspersky Security Center дерекқорында берілген; осы жалпыға ортақ көріністердің сипаттамасын klakdb.chm құжатынан таба аласыз).

Нәтижелер

Оқиғаларды SIEM жүйесіне экспорттауды конфигурациялағаннан кейін, экспорттағыңыз келетін оқиғаларды таңдаған болсаңыз, экспорт нәтижелерін қарай аласыз.

Алдын ала шарттар

Оқиғаларды Kaspersky Security Center-ге автоматты түрде экспорттауды конфигурациялау кезінде SIEM жүйесінің кейбір параметрлерін көрсету қажет. Kaspersky Security Center конфигурациялауға дайындалу үшін осы параметрлерді ертерек нақтылау ұсынылады.

Оқиғаларды SIEM жүйесіне автоматты түрде экспорттауды конфигурациялау үшін келесі параметрлердің мәндерін білу керек:

- **SIEM жүйелік серверінің мекенжайы**

  Қолданылатын SIEM жүйесі орнатылған сервердің мекенжайы. Бұл мәнді SIEM жүйесінің конфигурацияларында нақтылау керек.

- **SIEM жүйесінің сервер порты**

  Kaspersky Security Center және SIEM жүйесінің сервері арасында қосылым орнатылатын порт нөмірі. Бұл мәнді Kaspersky Security Center конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

- **Протокол**

  Хабарларды Kaspersky Security Center-ден SIEM жүйесіне жіберу үшін қолданылатын протокол. Бұл мәнді Kaspersky Security Center конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

Kaspersky Security Center-дегі оқиғалар туралы

Kaspersky Security Center бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады. Сіз осы ақпараты сыртқы SIEM жүйелеріне экспорттай аласыз. Оқиғалар туралы ақпаратты сыртқы SIEM жүйелеріне экспорттау арқасында SIEM жүйелерінің әкімшілері басқарылатын құрылғыларда немесе басқару топтарында орын алған қауіпсіздік жүйелерінің оқиғаларына тез арада ден қоя алатын болады.

Оқиға түрлері

Kaspersky Security Center-де хабарландырулардың келесі түрлері бар:

- Жалпы оқиғалар. Бұл оқиғалар барлық Kaspersky басқарылатын бағдарламаларында туындайды. Мысалы, Вирустық шабуыл жалпы оқиға. Жалпы оқиғалар қатаң белгіленген синтаксис пен семантикаға ие. Жалпы оқиғалар, мысалы, есептер мен мониторинг тақтасында қолданылады.
- Kaspersky басқарылатын бағдарламаларының айрықша оқиғалары. Kaspersky әрбір басқарылатын бағдарламасы өзіндік оқиғалар жиынтығына ие.

Оқиғалар көздері

Оқиғалар келесі бағдарламалар тарапынан жасалуы мүмкін:

- Kaspersky Security Center бағдарламасының құрамдастары:
  - Басқару сервері
  - Желілік агент
  - iOS MDM сервері
- Kaspersky басқарылатын бағдарламалары

  Kaspersky басқарылатын қолданбалары жасайтын оқиғалар туралы қосымша ақпарат тиісті қолданба құжаттамасында келтірілген.

Қолданба жасай алатын оқиғалардың толық тізімі қолданба саясатындағы **Оқиғаларды конфигурациялау** қойындысында келтірілген. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға болады.

Оқиғаның маңыздылық деңгейі

Әрбір оқиғаның өзіндік маңыздылық деңгейі бар. Туындау шарттарына байланысты, оқиғаға түрлі маңыздылық деңгейлері белгіленуі мүмкін. Оқиғалар маңыздылығының төрт деңгейі бар:

- *Критикалық оқиға* – деректерді жоғалтуға, жұмыстағы ақауға немесе критикалық қатеге әкелуі мүмкін критикалық мәселенің туындағанын білдіретін оқиға.

- *Функционалдық ақау* – бағдарламаның жұмысы немесе рәсімді орындау барысында туындаған күрделі мәселенің, қатенің немесе ақаудың орын алғанын білдіретін оқиға.

- *Ескерту* – міндетті түрде күрделі болып саналмаса да, болашақта мәселенің туындауы мүмкін екенін білдіретін оқиға. Оқиғалар туындағаннан кейін бағдарламаның жұмысы деректерді немесе функционалдық мүмкіндіктерді жоғалтпай қалпына келтіріле алса, осы оқиғалар көбінесе Ескертулерге қатысты болып келеді.

- *Ақпараттық хабарлар* – операцияның сәтті орындалуы, бағдарламаның дұрыс жұмыс істеуі немесе рәсімнің аяқталуы туралы хабарлау мақсатында туындайтын оқиға.

Әрбір оқиға үшін Kaspersky Security Center-де қарап шығуға немесе өзгертуге болатын сақтау уақыты белгіленген. Кейбір оқиғалар Басқару серверінің дерекқорында әдепкі бойынша сақталмайды, себебі олар үшін белгіленген уақыт нөлге тең. Сыртқы жүйелерге, Басқару серверінің дерекқорында кемінде бір күн бойы сақталатын оқиғалар ғана экспортталуы мүмкін.

Оқиғаларды экспорттау туралы

Сіз қауіпсіздік жүйелерінің мониторингін қамтамасыз ететін және әртүрлі шешімдерден деректерді шоғырландыратын ұйымдастырушылық және техникалық деңгейлерде қауіпсіздік мәселелерімен жұмыс істейтін орталықтандырылған жүйелерде оқиғалар экспортын қолдана аласыз. Оларға желілік аппараттық жасақтама мен қолданбалардың оқиғалары мен қауіпсіздік жүйелерінің ескертулерін нақты уақыт режимінде талдауды қамтамасыз ететін SIEM жүйелері, сондай-ақ қауіпсіздікті басқару орталықтары (Security Operation Center, SOC) қатысты болып келеді.

SIEM жүйелері деректерді көптеген көздерден, сонымен қатар желілерден, қауіпсіздік жүйелерінен, серверлерден, дерекқорлардан және қолданбалардан алады. Сондай-ақ, олар өңделген деректерді біріктіру функциясын қамтамасыз ете отырып, сізге критикалық оқиғаларды жіберіп алуға мүмкіндік бермейді. Бұдан бөлек, бұл жүйелер әкімшілерді дереу шешім қабылдауды талап ететін қауіпсіздік жүйесінің мәселелері туралы хабардар ету үшін дабыл сигналдары мен байланысты оқиғаларды автоматты талдауды орындайды. Хабарландырулар индикаторлар тақтасында көрсетілуі немесе бөгде арналар бойынша, мысалы, электрондық пошта арқылы таратылуы мүмкін.

Оқиғаларды Kaspersky Security Center-ден сыртқы SIEM жүйелеріне экспорттау рәсіміне екі тарап қатысады: оқиғаларды жіберуші – Kaspersky Security Center және оқиғаларды алушы – SIEM жүйесі. Оқиғаларды экспорттау сәтті аяқталуы үшін, мұны SIEM жүйесінде де, Kaspersky Security Center-де де конфигурациялау керек. Алдымен қай жағын конфигурациялағаныңыз маңызды емес. Kaspersky Security Center жүйесінде оқиғаларды жіберуді конфигурациялауға, содан кейін SIEM жүйесі арқылы оқиғаларды қабылдауды конфигурациялауға немесе керісінше орындауға болады.

Оқиғаларды Kaspersky Security Center-ден жіберу тәсілдерді

Оқиғаларды Kaspersky Security Center-ден сыртқы жүйелерге жіберудің үш тәсілі бар:

- Оқиғаларды Syslog протоколы бойынша кез келген SIEM жүйесіне жіберу.

  Syslog протоколы бойынша Kaspersky Security Center Басқару серверінде және басқарылатын құрылғыларды орнатылған Kaspersky бағдарламаларында орын алған кез келген оқиғаларды жіберуге болады. Syslog протоколы – хабарларды тіркеудің стандартты протоколы. Сіз осы протоколды оқиғаларды кез келген SIEM жүйесіне экспорттау үшін қолдана аласыз.

  Бұл үшін SIEM жүйесіне жібергіңіз келетін оқиғаларды белгілеу керек. Сіз оқиғаларды Басқару консолі немесе Kaspersky Security Center Web Console) көмегімен белгілей аласыз. SIEM жүйесіне тек белгіленген оқиғалар ғана жіберелетін болады. Сіз ештеңе белгілемеген болсаңыз, ешқандай оқиғалар жіберілмейді.

- Оқиғаларды QRadar, Splunk және ArcSight жүйелеріне CEF және LEEF протоколдары бойынша жіберу.

  CEF және LEEF протоколдарын жалпы оқиғаларды экспорттау үшін қолдануға болады. Оқиғаларды CEF және LEEF протоколдары бойынша экспорттау кезінде, белгіленген экспортталатын оқиғаларды таңдау мүмкіндігіңіз жоқ. Мұның орнына, барлық жалпы оқиғалардың экспорты орындалады. Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға түрлендіру үшін siem_conversion_rules.xml file файлын пайдалану қажет. Бұл файлда Kaspersky Security Center оқиға атрибуттарының тізімі және CEF және LEEF форматындағы оқиғалардың сәйкес атрибуттары бар. Сондай-ақ siem_conversion_rules.xml файлында оқиғаларға сәйкес хабарларды жасау ережелері бар. Бұл файл Kaspersky Security Center тарату жиынтығының құрамына кіреді.

  Syslog протоколынан айырмашылығы, CEF және LEEF протоколдары әмбебап болып саналады. CEF және LEEF протоколдары тиісті SIEM жүйелерге (QRadar, Splunk және ArcSight) арналған. Сол себепті, SIEM жүйесінде келесі протоколдардың бірі бойынша оқиғаларды экспорттауды таңдау кезінде қажетті талдағыш қолданылады.

- Тікелей Kaspersky Security Center дерекқорынан кез келген SIEM жүйесіне.

  Осы оқиғаларды экспорттау тәсілі, оқиғаларды SQL сұрауларының көмегімен дерекқордың көпшілікке қолжетімді көріністерінен тікелей алу үшін қолдануы мүмкін. Сұрау салу нәтижелері .xml файлына сақталады, оны сыртқы жүйеге арналған кіріс деректері ретінде қолдануға болады. Тікелей дерекқордан тек көпшілікке қолжетімді көріністерде қолжетімді оқиғаларды ғана экспорттауға болады.

SIEM жүйесінің оқиғаларды алуы

SIEM жүйесі Kaspersky Security Center-ден алынатын оқиғаларды қабылдауы және дұрыс талдауы тиіс. Бұл үшін SIEM жүйесін конфигурациялауды орындау керек. Конфигурация нақты қолданылатын SIEM жүйесіне байланысты болып келеді. Алайда, барлық SIEM жүйелерінің конфигурацияларында қабылдағыш пен талдағышты конфигурациялау сияқты бірқатар жалпы кезеңдер бар.

Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау туралы

Оқиғаларды Kaspersky Security Center-ден сыртқы SIEM жүйелеріне экспорттау рәсіміне екі тарап қатысады: оқиғаларды жіберуші – Kaspersky Security Center және оқиғаларды алушы – SIEM жүйесі. Оқиғаларды экспорттау, қолданылатын SIEM жүйесінде және Kaspersky Security Center-де конфигурациялануы керек.

SIEM жүйесінде орындалатын конфигурациялар сіз қолданатын жүйеге байланысты болып келеді. Жалпы жағдайда, алынған хабарларды өрістерге жаю үшін, барлық SIEM жүйелеріне хабар қабылдағышты және қажет болса, хабар талдағышты конфигурациялау керек.

Хабар қабылдағышты конфигурациялау

SIEM жүйесі үшін Kaspersky Security Center жіберетін оқиғаларды қабылдау үшін қабылдағышты конфигурациялау қажет. Жалпы жағдайда, SIEM жүйесінде келесі параметрлерді көрсету керек:

- **Экспорттау протоколы немесе кіріс деректері түрі**

  Бұл хабарлама жіберу протоколы, мысалы, UDP. Kaspersky Security Center-де оқиғаларды жіберу үшін таңдалған протоколды көрсету керек.

- **Порт**

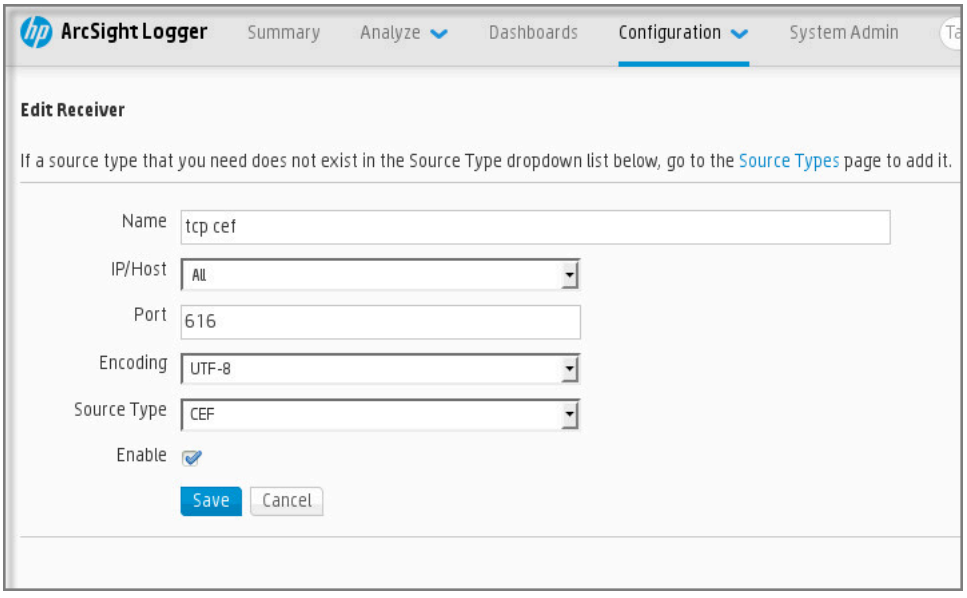
  Kaspersky Security Center-ге қосылуға арналған порт нөмірі. Kaspersky Security Center-де оқиғаларды жіберу үшін таңдалған порт нөмірін көрсету керек.

- **Хабар жіберу протоколы немесе шығыс деректері түрі**

  Оқиғаларды SIEM жүйесіне экспорттау үшін қолданылатын протокол. Бұл келесі стандарттың протоколдардың бірі болуы мүмкін: Syslog, CEF немесе LEEF. SIEM жүйесі аталған протоколға сай келетін оқиғалар талдағышын таңдайды.

Қолданылатын SIEM жүйесіне байланысты, хабар қабылдағыштың қосымша параметрлерін көрсету қажет болуы мүмкін.

Төмендегі суретте, қабылдағышты ArcSight-та конфигурациялау мысалы келтірілген.



Қабылдағышты ArcSight-та конфигурациялау

Хабарлар талдағышы

Экспортталатын оқиғалар SIEM жүйесіне хабарлар түрінде беріледі. Содан соң, оқиғалар туралы ақпарат SIEM жүйесіне тиісінше берілуі үшін, осы хабарларға талдағыш қолданылады. Хабарлар талдағышы SIEM жүйесіне кіріктірілген; ол хабарды хабар идентификаторы, маңыздылық деңгейі, сипаттамасы, параметрлері сияқты өрістерге бөлу үшін қолданылады. Нәтижесінде, SIEM жүйесі Kaspersky Security Center-ден алынған оқиғаларды SIEM жүйесінің дерекқорында сақталатындай етіп өңдеу мүмкіндігіне ие.

SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау

Оқиғаларды автоматты түрде экспорттауды қосқаннан кейін, сыртқы SIEM жүйесіне қандай оқиғалар экспортталатынын таңдау керек.

Оқиғаларды Syslog пішімінде келесі шарттардың біріне негізделген сыртқы жүйеге экспорттауды конфигурациялауға болады:

- Жалпы оқиғаларды таңдау. Егер сіз саясатта, оқиғаның сипаттарында немесе Басқару сервері сипаттарында экспортталатын оқиғаларды таңдасаңыз, онда осы саясатпен басқарылатын барлық бағдарламаларда орын алған таңдалған оқиғалар SIEM жүйесіне жіберіледі. Егер экспортталатын оқиғалар саясатта таңдалған болса, сіз осы саясатпен басқарылатын жеке бағдарлама үшін оларды қайта анықтай алмайсыз.

- Басқарылатын бағдарлама үшін оқиғаларды таңдау. Егер сіз басқарылатын құрылғыларда орнатылған басқарылатын бағдарлама үшін экспортталатын оқиғаларды таңдасаңыз, онда SIEM жүйесіне тек осы бағдарламада орын алған оқиғалар ғана жіберіледі.

Syslog пішімінде экспорттау үшін Kaspersky қолданбасы оқиғаларын жасау

Егер сіз басқарылатын құрылғыда орнатылған бөлек басқарылатын бағдарламада болған оқиғаларды экспорттағыңыз келсе, бағдарлама үшін экспортталатын оқиғаларды таңдаңыз. Егер экспортталатын оқиғалар бұған дейін саясатта таңдалған болса, сіз осы саясатпен басқарылатын жеке бағдарлама үшін таңдалған оқиғаларды қайта анықтай алмайсыз.

Жеке басқарылатын бағдарламаға арналған оқиғаларды таңдау үшін:

1. Kaspersky Security Center консолі шежіресінде **Басқарылатын құрылғылар** түйінін таңдап, **Құрылғылар** қойыншасына өтіңіз.

2. Тінтуірдің оң жақ түймесімен қажетті құрылғының мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

3. Ашылған құрылғының сипаттар терезесінде **Бағдарламалар** бөлімін таңдаңыз.

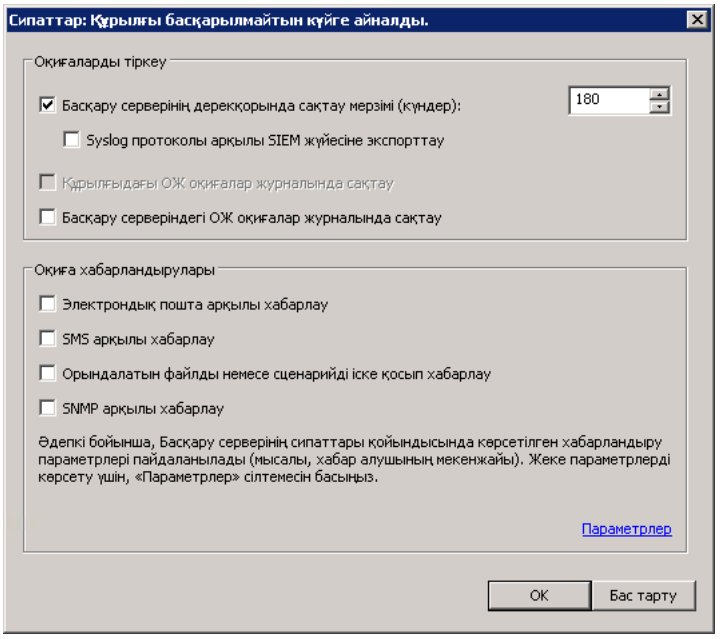
4. Пайда болған бағдарламалар тізімінен оқиғаларды экспорттауды қажет ететін бағдарламаны таңдап, **Сипаттар** түймесін басыңыз.

5. Бағдарлама сипаттары терезесінде **Оқиғаларды конфигурациялау** бөлімін таңдаңыз.

6. Пайда болған оқиғалар тізімінен SIEM жүйесіне экспорттау қажет бір немесе бірнеше оқиғаны таңдап, **Сипаттар** түймесін басыңыз.

7. Syslog пішімінде экспорттау мақсатында, таңдалған оқиғаларды белгілеу үшін ашылған оқиға сипаттары терезесінде **Syslog протоколы арқылы SIEM жүйесіне экспорттау** параметрін таңдаңыз. Syslog пішімінде экспортталатын оқиғаларды таңдауды болдырмау үшін **Syslog протоколы арқылы SIEM жүйесіне экспорттау** параметрін өшіріңіз.

Егер оқиға сипаттары саясатта орнатылса, сол терезенің өрістерін өңдеу мүмкін емес.



Оқиғалар сипаттары терезесі

8. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

9. Бағдарлама сипаттары терезесі мен құрылғы сипаттары терезесінде **OK** түймесін басыңыз.

Таңдалған оқиғалар SIEM жүйесіне Syslog пішімінде жіберілетін болады. Сіз **Syslog протоколы арқылы SIEM жүйесіне экспорттау** параметрімен болдырмаған оқиғалар SIEM жүйесіне экспортталмайды. Автоматты экспорттауды қосып, экспортталатын оқиғаларды таңдағаннан кейін экспорттау бірден басталады. Оқиғаларды Kaspersky Security Center-ден алуды қамтамасыз ету үшін SIEM жүйесін конфигурациялаңыз.

Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау

Егер сіз белгілі бір саясатпен басқарылатын барлық бағдарламаларда болған оқиғаларды экспорттағыңыз келсе, саясатта экспортталатын оқиғаларды таңдаңыз. Бұл жағдайда, сіз жеке басқарылатын бағдарлама үшін оқиғаларды таңдай алмайсыз.

SIEM жүйесіне экспортталатын жалпы оқиғаларды таңдау үшін:

1. Kaspersky Security Center консолі шежіресінде **Саясаттар** түйінін таңдаңыз.

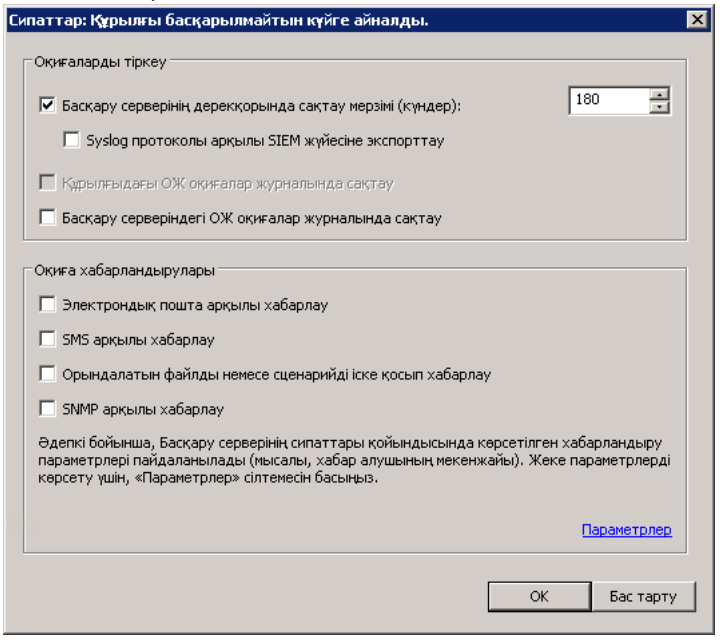
2. Тінтуірдің оң жақ түймесімен қажетті саясаттың мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

3. Ашылған саясат сипаттары терезесінде **Оқиғаларды конфигурациялау** бөлімін таңдаңыз.

4. Пайда болған оқиғалар тізімінен SIEM жүйесіне экспорттау қажет бір немесе бірнеше оқиғаны таңдап, **Сипаттар** түймесін басыңыз.

   Барлық оқиғаларды таңдау керек болса, **Барлығын таңдау** түймесін басыңыз.

5. Syslog пішімінде экспорттау мақсатында, таңдалған оқиғаларды белгілеу үшін ашылған оқиға сипаттары терезесінде **Syslog протоколы арқылы SIEM жүйесіне экспорттау** параметрін таңдаңыз. Syslog пішімінде экспортталатын оқиғаларды таңдауды болдырмау үшін **Syslog протоколы арқылы SIEM жүйесіне экспорттау** жалаушасын алып тастаңыз.



Басқару сервері оқиғалары сипаттары терезесі

6. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

7. Саясат сипаттары терезесінде **OK** түймесін басыңыз.

Таңдалған оқиғалар SIEM жүйесіне Syslog пішімінде жіберілетін болады. Сіз **Syslog протоколы арқылы SIEM жүйесіне экспорттау** параметрімен болдырмаған оқиғалар SIEM жүйесіне экспортталмайды. Автоматты экспорттауды қосып, экспортталатын оқиғаларды таңдағаннан кейін экспорттау бірден басталады. Оқиғаларды Kaspersky Security Center-ден алуды қамтамасыз ету үшін SIEM жүйесін конфигурациялаңыз.

Syslog пішіміндегі оқиғаларды экспорттау туралы

Syslog пішімін қолдана отырып, басқарылатын құрылғыларда орнатылған Kaspersky Басқару сервері мен басқа да бағдарламаларында орын алған оқиғаларды SIEM жүйелеріне экспорттауға болады.

Syslog – бұл хабарларды тіркеудің стандартты протоколы. Бұл протокол, хабарды құрастыратын бағдарламалық жасақтаманы, хабарлар сақталатын жүйені және хабарлар бойынша талдау мен есептілікті орындайтын бағдарламалық жасақтаманы бөлуге мүмкіндік береді. Әрбір хабарға, хабар құрастырылған бағдарламалық жасақтаманың түрін көрсететін құрылғының коды және маңыздылық деңгейі беріледі.

Syslog пішімі Internet Engineering Task Force жариялаған Request for Comments (RFC) құжаттарымен айқындалады. RFC 5424 стандарты оқиғаларды Kaspersky Security Center-ден сыртқы жүйелерге экспорттау үшін қолданылады.

Kaspersky Security Center-де оқиғаларды Syslog пішімінде сыртқы жүйелерге экспорттауды конфигурациялауға болады.

Экспорттау процесі екі қадамнан тұрады:

1. Оқиғаларды автоматты түрде экспорттауды қосу. Бұл қадамда Kaspersky Security Center бағдарламасы, оқиғалар SIEM жүйесіне жіберілетіндей етіп конфигурацияланады. Автоматты түрде экспорттау қосылғаннан кейін, Kaspersky Security Center-ден оқиғаларды жіберу бірден басталады.

2. Сыртқы жүйеге экспортталатын оқиғаларды таңдау. Бұл қадамда қандай оқиғалардың SIEM жүйесіне экспортталтанын таңдау керек.

CEF және LEEF пішіміндегі оқиғаларды экспорттау туралы

CEF және LEEF пішімдерін, SIEM жүйесіне жалпы оқиғаларды, сондай-ақ Kaspersky бағдарламалары Басқару серверіне жіберген оқиғаларды экспорттау үшін пайдалануға болады. Экспортталатын оқиғалар жиынтығы алдын ала анықталған, экспортталатын оқиғаларды таңдау мүмкіндігі жоқ. Оқиғаларды SIEM жүйесіне (QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет.

Экспорттау пішімін, сіз қолданатын SIEM жүйесіне байланысты таңдауға болады. Келесі кестеде SIEM жүйелері және оларға сәйкес экспорттау пішімдері келтірілген.

Оқиғаларды SIEM жүйесіне экспорттау пішімдері

SIEM жүйесі	Экспорттау пішімі
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) — IBM Security QRadar SIEM үшін реттелген оқиға пішімі. QRadar платформасы LEEF оқиғаларын ендіріп, анықтап, өңдей алады. LEEF протоколы үшін UTF-8 кодтамасы қолданылуы керек. LEEF протоколы туралы толығырақ ақпаратты IBM Knowledge Center веб-бетінен қараңыз.

- CEF – бұл әртүрлі желілік құрылғылар мен қолданбалардың қауіпсіздік жүйесі ақпаратының үйлесімділігін жақсартатын "ашық журнал" типті басқару стандарты. CEF протоколы, кәсіпорынды басқару жүйелері талдауға арналған деректерді оңай алуы және біріктіруі үшін оқиғалар журналының жалпы пішімін пайдалануға мүмкіндік береді. CEF протоколы үшін UTF-8 кодтамасы қолданылуы керек.

Автоматты түрде экспорттау кезінде Kaspersky Security Center жалпы оқиғаларды SIEM жүйесіне жібереді. Оқиғаларды автоматты түрде экспорттау қосылғаннан кейін бірден басталады. Бұл бөлімде оқиғаларды автоматты түрде экспорттауды қосу рәсімі сипатталған.

Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center конфигурациялау

Оқиғаларды автоматты түрде Kaspersky Security Center-ге экспорттауды қосуға болады.

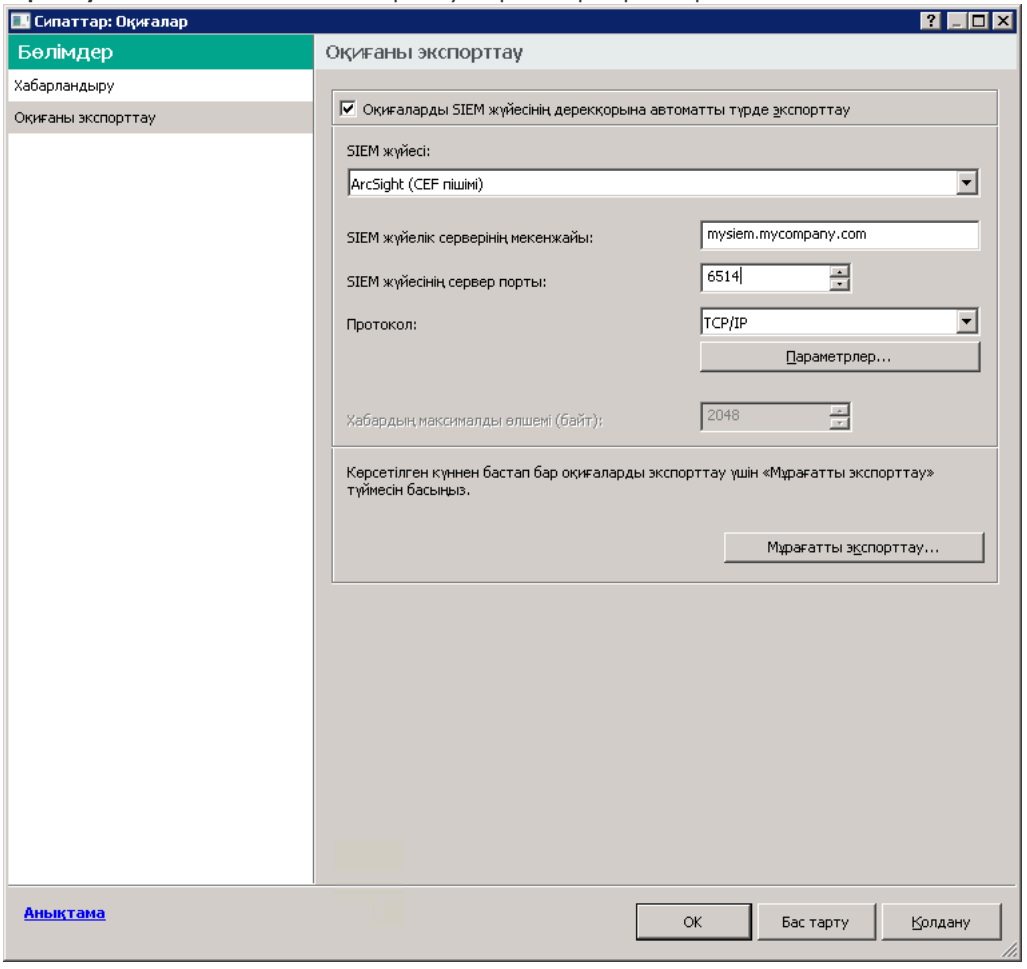
Тек жалпы оқиғаларды басқарылатын бағдарламалардан CEF және LEEF пішіміндерінде экспорттауға болады. Оқиғаларды CEF және LEEF форматына түрлендіру үшін қолданылатын интерпретациялау ережелері Kaspersky Security Center тарату жинағына кіретін siem_conversion_rules.xml файлында көрсетілген. Бағдарламаның айрықша оқиғаларын басқарылатын бағдарламалардан CEF және LEEF пішімдерінде экспорттау мүмкін емес. Басқарылатын бағдарлама оқиғаларын немесе басқарылатын бағдарлама саясаты арқылы конфигурацияланған пайдаланушы оқиғалары жиынтығын экспорттау қажет болса, Syslog пішімінде оқиғаларды экспорттауды пайдаланыңыз.

Жалпы оқиғаларды автоматты түрде экспорттауды қосу үшін:

1. Kaspersky Security Center консоль ағашында оқиғаларды экспорттау қажет Басқару сервері деп аталатын түйінді таңдаңыз.
2. Таңдалған Басқару серверінің жұмыс аймағында **Оқиғалар** қойыншасына өтіңіз.
3. **Хабарландырулар мен оқиғаларды экспорттау параметрлерін конфигурациялау** сілтемесінің жанындағы ашылмалы көрсеткіні басып, ашылмалы тізімнен **SIEM жүйесіне экспорттауды теңшеу** опциясын таңдаңыз.

   Оқиғаны экспорттау бөліміндегі оқиғалар сипаттары терезесі ашылады.

4. **Оқиғаны экспорттау** бөлімінде келесі экспорттау параметрлерін көрсетіңіз:



Оқиғалар сипаттары терезесі Оқиғаларды экспорттау бөлімі

- **Оқиғаларды SIEM жүйесінің дерекқорына автоматты түрде экспорттау**

  Оқиғаларды SIEM жүйесіне автоматты түрде экспорттауды қосу үшін осы жалаушаны қойыңыз. Бұл жалаушаны қойғанда, **Оқиғаларды экспорттау** бөліміндегі барлық өрістер өңдеуге қолжетімді болады.

- **SIEM жүйесі**

  Оқиғаларды экспорттау үшін SIEM жүйесін таңдаңыз: QRadar® (LEEF пішімі), ArcSight (CEF пішімі), Splunk® (CEF пішімі) және Syslog пішімі (RFC 5424).

  Syslog форматын таңдасаңыз, сізге мынаны көрсету керек:

  Хабардың максималды өлшемі (байт)

  SIEM жүйесіне жіберілетін бір хабардың байтындағы максималды өлшемді көрсетіңіз. Әр оқиға бір хабармен беріледі. Егер хабардың нақты ұзындығы көрсетілген мәннен асып кетсе, хабар кесіліп, деректер жоғалуы мүмкін. Хабардың әдепкі өлшемі 2048 байтты құрайды. Бұл өріс, **SIEM жүйесі** өрісінде Syslog пішімін таңдаған болсаңыз ғана қолжетімді.

- **SIEM жүйелік серверінің мекенжайы**

  SIEM жүйелік серверінің мекенжайын көрсетіңіз. Сервер мекенжайын DNS немесе NetBIOS атауы немесе IP мекенжайы ретінде көрсетуге болады.

- **SIEM жүйесінің сервер порты**

  SIEM жүйесі серверіне қосылу үшін порт нөмірін көрсетіңіз. Бұл порт нөмірі оқиғаларды алу үшін SIEM жүйесі қабылдағышының параметрлерінде көрсетілген порт нөміріне сәйкес келуі керек (SIEM жүйесін конфигурациялау бөлімін қараңыз).

- **Протокол**

  SIEM жүйесіне хабар жіберу протоколын таңдаңыз. TCP протоколының орнына TCP, UDP немесе TLS таңдауға болады.

  TLS over TCP таңдасаңыз, келесі TLS параметрлерін көрсетіңіз:

  - **SIEM серверінің аутентификациясы**

    SIEM жүйесі серверінің түпнұсқалық растамасының келесі тәсілдерінің бірін таңдаңыз:

    - **CA сертификаттарын пайдалану арқылы**. Сертификаттар тізімі бар файлды сенімді сертификаттау орталығынан (CA) ала аласыз және оны Kaspersky Security Center бағдарламасына жүктей аласыз. Kaspersky Security Center бағдарламасы SIEM жүйесінің сертификатына сенімді сертификаттау орталығы қол қойғанын не қол қоймағанын тексереді.

      Сенімді сертификатты қосу үшін **Шолу** түймесін басып, сертификатты жүктеп алыңыз.

      CA сертификаттарын пайдалану арқылы параметрін таңдасаңыз, **Сервер сертификаттарының тақырыптары (міндетті емес)** өрісінде субъектілер аттарын көрсетуге болады. *Субъект атауы* – сертификат алуға себеп болған домендік атау. SIEM жүйесі серверінің домендік атауы SIEM жүйесінің сервері сертификаты субъектісінің атына сәйкес келмесе, Kaspersky Security Center бағдарламасы SIEM жүйесінің серверіне қосыла алмайды. Алайда, сертификатта субъектінің атауы өзгерген жағдайда, SIEM жүйесінің сервері өзінің домендік атауын өзгерте алады. Бұл үшін, **Сервер сертификаттарының тақырыптары (міндетті емес)** өрісінде субъектілердің аттарын көрсетіңіз. Егер аталған субъектілердің кез келгені SIEM жүйесі сертификаты субъектісінің атына сәйкес келсе, Kaspersky Security Center бағдарламасы SIEM жүйесі серверінің сертификатын тексереді.

    - **Сервер сертификаттарының SHA1 саусақ& іздерін қолдану арқылы**. Kaspersky Security Center SHA-1 бағдарламасында SIEM жүйесі сертификаттарының сәйкестендіру белгілерін көрсете аласыз. SHA-1 сәйкестендіру белгісін қосу үшін оны параметрдің астындағы өріске енгізіңіз.

  - **Клиенттік аутентификация**

Клиенттің түпнұсқалық растамасы үшін сіз өзіңіздің сертификатыңызды енгізе аласыз немесе оны Kaspersky Security Center бағдарламасында жасай аласыз.

- **Сертификатты салу**. Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Бұрыннан бар сертификатты енгізу үшін **Сертификатты шолу** түймесін басыңыз. Ашылған **Сертификат** терезесінде келесі сертификат түрлерінің бірін таңдаңыз, содан кейін сертификат пен оның жеке кілтін көрсетіңіз:

  - **X.509 сертификаты**. **Жабық кілт (*.prk, *.pem)** өрісіне жеке кілт файлын және **Сертификат (*.cer)** өрісіне сертификаты бар файлды жүктеңіз. Ол үшін тиісті өрістің оң жағындағы **Шолу** түймесін басып, қажетті файлды қосыңыз. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде, **Құпиясөз** өрісінде жеке кілтті шифрсыздау үшін құпиясөзді енгізіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

  - **PKCS #12 контейнері**. Сертификат пен оның жеке кілтін қамтитын бір файлды **Сертификат файлы** өрісіне жүктеңіз. Ол үшін өрістің оң жағындағы **Шолу** түймесін басып, қажетті файлды қосыңыз. Файл жүктелгеннен кейін, **Құпиясөз** өрісінде жеке кілтті шифрсыздау үшін құпиясөзді көрсетіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- **Кілті жасау**. Сіз Kaspersky Security Center бағдарламасында өзіне қол қойылған сертификатты жасай аласыз. **Сертификат жасау** түймесін басып, **Тақырып** өрісінде субъект атауын енгізіңіз. Пайдаланушы сертификаты осы субъект атауы үшін жасалады және осы сертификаттың SHA-1 сәйкестендіру белгісі **Клиент сертификатының SHA1 саусақ ізі** өрісінде көрсетіледі. Нәтижесінде, Kaspersky Security Center өзіне қол қойылған сертификатты сақтайды және сіз сертификаттың жария бөлігін немесе SHA-1 сәйкестендіру белгісін SIEM жүйесіне жібере аласыз.

5. Егер өткендегі белгілі бір күннен кейін орын алған оқиғаларды SIEM жүйесіне экспорттау қажет болса, **Мұрағатты экспорттау** түймесін басып, оқиғаны экспорттау басталатын күнді көрсетіңіз. Әдепкі бойынша, оқиғаларды экспорттау қосылғаннан кейін бірден басталады.

6. SIEM жүйесінің байланысы сәтті конфигурацияланғанына көз жеткізу үшін **Параметрлерді сынау** түймесін басыңыз.

   Қолданба SIEM жүйелік серверімен байланыс орнатуға және сынақ оқиғасын жіберуге тырысады. Байланыс орнатылмаса, қате туралы хабар көрсетіледі. Байланыс орнатылса, ешқандай хабар көрсетілмейді. Қажет болса, сынақ оқиғасын **Оқиғалар** қойындысынан көруге болады.

7. **OK** түймесін басыңыз.

Оқиғаларды автоматты түрде экспорттау қосылған.

Оқиғаларды автоматты түрде экспорттауды қосқаннан кейін, SIEM жүйесіне қандай оқиғалар экспортталатынын таңдау керек.

Оқиғаларды тікелей дерекқордан экспорттау

Kaspersky Security Center интерфейсін пайдаланбай-ақ, оқиғаларды тікелей Kaspersky Security Center дерекқорынан алуға болады. Тікелей жария көріністерге сұраулар жасауға және олардан оқиғалар туралы деректерді алуға немесе бұрыннан бар жария көріністер негізінде өзіндік көріністер жасауға және қажетті деректерді алу үшін оларға жүгінуге болады.

Жария көріністер

Сізге ыңғайлы болу үшін, Kaspersky Security Center дерекқорында жария көріністер жиынтығы қарастырылған. Жария ұсыныстардың сипаттамасы klakdb.chm құжатында келтірілген.

v_akpub_ev_event жария көрінісі дерекқордағы оқиғалар параметрлеріне сәйкес келетін өрістер жиынтығын қамтиды. klakdb.chm құжатында Kaspersky Security Center-дің басқа нысандарына, мысалы, құрылғыларға, бағдарламаларға, пайдаланушыларға қатысты жария көріністер туралы ақпарат та бар. Сіз бұл ақпаратты сұраулар жасау кезінде пайдалана аласыз.

Бұл бөлімде klsql2 утилитасы арқылы SQL сұрауын жасау нұсқаулары, сондай-ақ осындай сұраудың мысалы берілген.

Сондай-ақ, SQL сұраулары мен дерекқор көріністерін жасау үшін дерекқорлармен жұмыс істеуге арналған кез келген басқа бағдарламаларды пайдалануға болады. Kaspersky Security Center дерекқорына қосылу параметрлерін, мысалы, дананың атауын және дерекқордың атауын қалай қарау керектігі туралы ақпарат тиісті бөлімде берілген.

klsql2 утилитасы арқылы SQL сұрауын жасау

Бұл мақалада klsql2 утилитасын жүктеп алу және пайдалану, сондай-ақ осы утилита арқылы SQL сұрауын жасау туралы нұсқаулар берілген.

klsql2 утилитасын пайдалану үшін:

1. klsql2 утилитасын Kaspersky Security Center орнату қалтасынан табыңыз. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Kaspersky Security Center бағдарламасының ескі нұсқаларына арналған klsql2 утилитасының нұсқаларын пайдаланбаңыз.

2. Кез келген мәтін редакторында .sql кеңейтімі бар файл жасаңыз да, файлды утилитасы бар сол қалтаға салыңыз.

3. .sql файлында қажетті SQL сұрауын теріп, файлды сақтаңыз.

4. Kaspersky Security Center басқару сервері орнатылған құрылғыда .sql файлынан SQL сұрауын іске қосу және нәтижелерді result.xml файлына сақтау үшін келесі пәрменді теріңіз:

   ```
   klsql2 -i src.sql -u <пайдаланушы аты> -p <құпиясөз> -o result.xml
   ```

   мұндағы <пайдаланушы аты> және <құпия сөз> дерекқорға рұқсаты бар пайдаланушы есептік жазбасының есептік деректері болып табылады.

5. Қажет болса, дерекқорға қатынасуға рұқсаты бар пайдаланушының есептік жазбасының атауы мен құпиясөзін енгізіңіз.

6. Жаңадан жасалған result.xml файлдарын ашып, SQL сұрау нәтижелерін қараңыз.

.sql файлын өңдей аласыз және кез келген SQL сұрауын жалпыға жария жасай аласыз. Содан кейін, пәрмен жолындағы пәрменді пайдаланып, SQL сұрауын іске қосып, нәтижелерді файлға сақтауға болады.

klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы

Бұл бөлімде klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы көрсетілген.

Келесі мысалдарда құрылғыларда соңғы жеті күнде орын алған оқиғаларды шығарып алу және пайда болған уақытына байланысты ретімен берілген оқиғалар берілген. Ең соңғы оқиғалар бірінші көрсетіледі.

Microsoft SQL серверінің мысалы:

```
SELECT
  /* оқиға идентификаторы */
  e.nId,

  /* оқиға болған уақыт */
  e.tmRiseTime,

  /* оқиға түрінің ішкі атауы */
  e.strEventType,

  /* оқиғаның көрсетілген атауы */
  e.wstrEventTypeDisplayName,

  /* оқиғаның көрсетілген сипаттамасы */
  e.wstrDescription,

  /* құрылғы орналасқан топтың атауы */
  e.wstrGroupName,

  /* оқиға орын алған құрылғының көрсетілген атауы */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* оқиға орын алған құрылғының IP мекенжайы */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

PostgreSQL мысалы:

```
SELECT
  /* оқиға идентификаторы */
  "e"."nId",

  /* оқиға болған уақыт */
  "e"."tmRiseTime",

  /* оқиға түрінің ішкі атауы */
  "e"."strEventType",

  /* оқиғаның көрсетілген атауы */
  "e"."wstrEventTypeDisplayName",

  /* оқиғаның көрсетілген сипаттамасы */
  "e"."wstrDescription",

  /* оқиғаның көрсетілген сипаттамасы */
  "e"."wstrGroupName",

  /* оқиға орын алған құрылғының көрсетілген атауы */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* оқиға орын алған құрылғының IP мекенжайы */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL немесе MariaDB мысалы:

```
SELECT

  /* оқиға идентификаторы */
  `e`.`nId`,

  /* оқиға болған уақыт */
  `e`.`tmRiseTime`,

  /* оқиға түрінің ішкі атауы */
  `e`.`strEventType`,

  /* оқиғаның көрсетілген атауы */
  `e`.`wstrEventTypeDisplayName`,

  /* оқиғаның көрсетілген сипаттамасы */
  `e`.`wstrDescription`,

  /* құрылғы тобының атауы */
  `e`.`wstrGroupName`,

  /* оқиға орын алған құрылғының көрсетілген атауы */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* оқиға орын алған құрылғының IP мекенжайы */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Kaspersky Security Center дерекқорының атауын қарау

Мысалы, SQL сұрауын жіберу және SQL скрипттер редакторынан дерекқорға қосылу қажет болса, дерекқордың атауын білу пайдалы болуы мүмкін.

Kaspersky Security Center дерекқорының атауын көру үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

2. Басқару сервері сипаттары терезесінде **Кеңейтілген** бөлімін, содан соң **Ағымдағы дерекқор мәліметтері** тармағын таңдаңыз.

3. **Ағымдағы дерекқор мәліметтері** бөлімінде дерекқордың келесі сипаттарына назар аударыңыз (төмендегі суретті қараңыз):

   - **Үлгінің атауы**

     Пайдаланылатын Kaspersky Security Center дерекқоры үлгісінің атауы. Әдепкі бойынша мәні – *.\KAV_CS_ADMIN_KIT.*

   - **Дерекқор атауы**

     Kaspersky Security Center SQL дерекқоры атауы. Әдепкі бойынша, *KAV* мәні көрсетілген.

   - **Kaspersky Security Center дерекқоры үшін бөлінген орын**

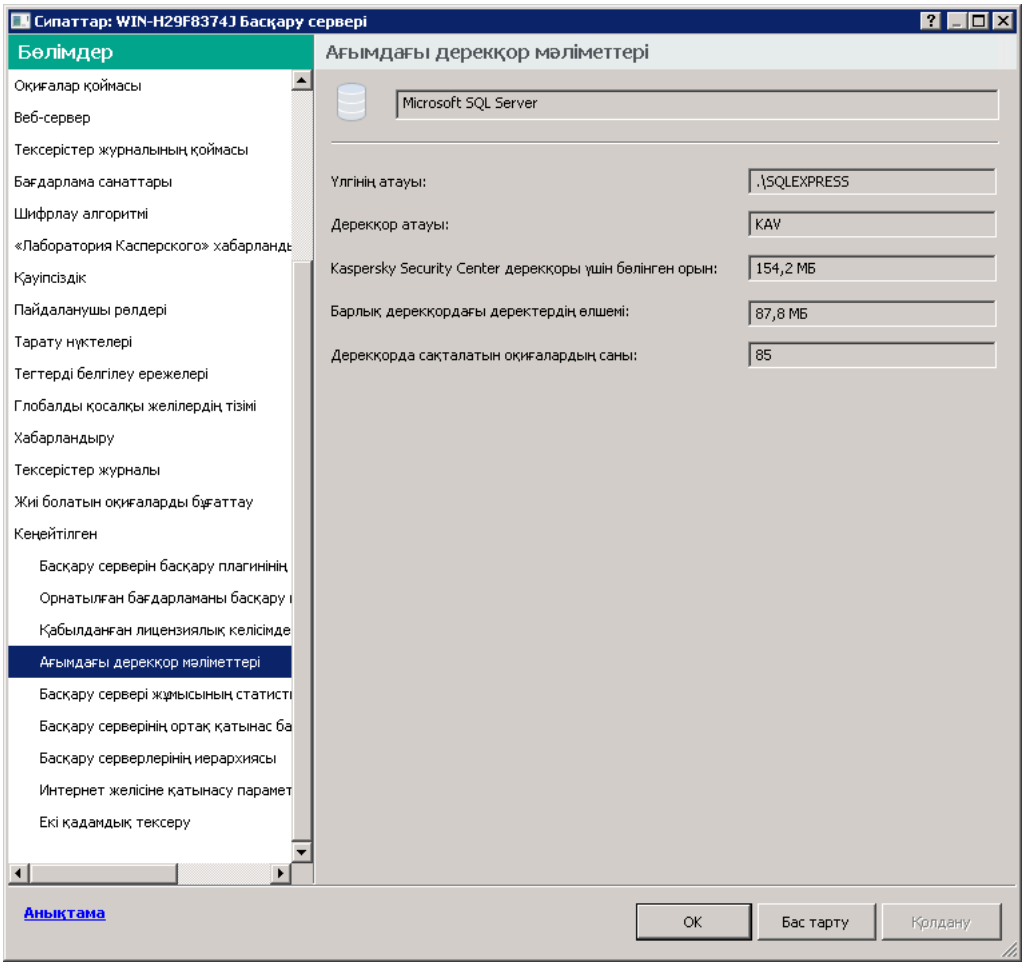
     Дерекқор файлының өлшемі. Қажетсіз деректерді тазалау қажет болса, *Басқару серверіне техникалық қызмет көрсету* тапсырмасы көмегімен дерекқорды қысуды конфигурациялаңыз.

   - **Барлық дерекқордағы деректердің өлшемі**

     ДҚБЖ-да қазір қолданылып жатқан деректердің нақты өлшемі. Келесі мақалада ДҚБЖ-ны диагностикалау әдісі сипатталған: Дерекқор өлшемі шектен асады.

- **Дерекқорда сақталатын оқиғалардың саны**

  Қазіргі уақытта ДҚБЖ-ға сақталған оқиғалар саны. Мәліметтер алу үшін келесі мақаланы қараңыз: Оқиғаны өңдеу және сақтау.



Басқару серверінің ағымдағы дерекқор мәліметтері бар бөлім

4. Басқару сервері сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

SQL сұрауларында дерекқорға қосылу және жүгіну үшін осы дерекқор атауын пайдаланыңыз.

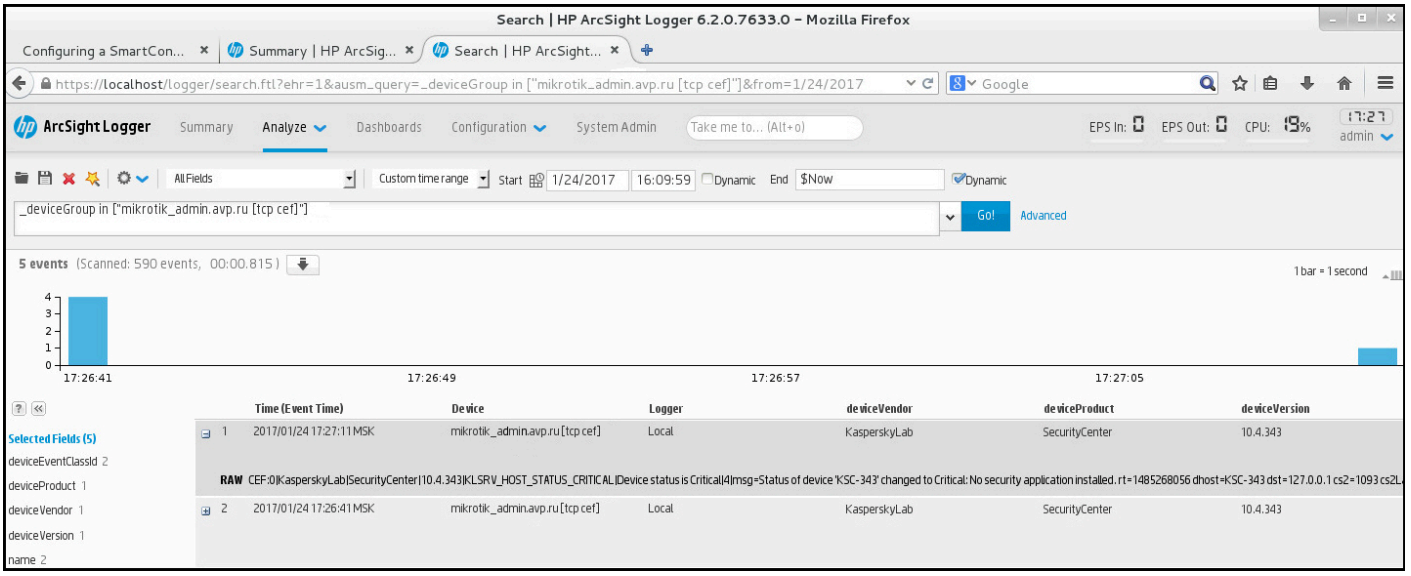
Экспорт нәтижелерін қарау

Экспорттау рәсімі сәтті аяқталғанын білуіңізге болады. Бұл үшін SIEM жүйесі экспортталатын оқиғаларды қамтитын хабарларды алып-алмағанын тексеріңіз.

Kaspersky Security Center-ден жіберілген оқиғаларды SIEM жүйесі алып, дұрыс түсіндірсе, онда екі жақтағы конфигурациялау дұрыс орындалды. Әйтпесе, Kaspersky Security Center және SIEM жүйесінің конфигурациясын тексеріп, қажет болған жағдайда түзетіңіз.

Төменде ArcSight жүйесіне экспортталған оқиғалардың мысалы келтірілген. Мысалы, бірінші оқиға – Басқару серверінің критикалық оқиғасы: *Құрылғының күйі "Критикалық"*.

Экспортталған оқиғалардың көрсетілуі қолданылатын SIEM жүйесіне байланысты.



Оқиғалар мысалы

Статистиканы үшінші тарап бағдарламаларына жіберу үшін SNMP пайдалану

Бұл бөлімде Windows-тағы SNMP протоколы арқылы Басқару серверінен ақпаратты қалай алуға болатыны сипатталады. Kaspersky Security Center бағдарламасы, Басқару сервері жұмысының статистикасын OID көмегімен үшінші тарап бағдарламаларына беретін SNMP агентін қамтиды.

Бұл бөлімде, Kaspersky Security Center үшін SNMP қолдану кезінде туындауы мүмкін мәселелерді шешуге бағытталған әрекеттер туралы ақпарат та бар.

SNMP қызметін Kaspersky Security Center-мен пайдалану үшін конфигурациялау

Бұл бөлім Simple Network Management Protocol (SNMP) пайдаланып Басқару серверінен ақпаратты алу үшін Windows жүйесінде SNMP қызметін конфигурациялау жолын сипаттайды.

Әдепкі бойынша, Windows жүйесінде SNMP қолдауы өшірілген.

Windows жүйесінде SNMP қолдауын қосу үшін:

1. **Басқару тақтасына** өтіңіз.
2. **Бағдарламаларды орнату және жою** мәзірін ашыңыз.
3. **Windows құрамдастарын қосу немесе өшіру** түймесін басыңыз.
4. Windows мүмкіндіктерінің тізімінде SNMP мүмкіндігіне өтіп, **OK** түймесін басыңыз.
5. **Басқару тақтасы** → **Басқару** → **Қызметтер** тармағына өтіңіз.

6. **SNMP қызметін** таңдап, іске қосыңыз.

7. UPD порты үшін `netstat` көмегімен тексеріп, тыңдаудың жұмыс істеп тұрғанын тексеріңіз.

SNMP қолдауы Windows жүйесінде қосылған.

Windows жүйесінде SNMP қызметін конфигурациялау үшін:

1. Kaspersky Security Center **SNMP агенті** құрамдасы әдеттегі немесе дыбыссыз орнату кезінде орнатылғанына көз жеткізіңіз.

2. **SNMP қызметі** мен Windows **SNMP-тұзақ қызметі** іске қосылғанына көз жеткізіңіз.

3. Жүйеде MIB Browser ManageEngine орнатылғанын тексеріңіз.

4. **Қауіпсіздік** қойындысындағы **SNMP қызметінің** сипаттарында келесі құқықтары бар екі қоғамдастықты қосыңыз:

Қоғамдастық	Құқықтар
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. **Осы құрылғылардан SNMP пакеттерін алу** өрісіне ManageEngine MIB шолғышы орнатылған құрылғының IP мекенжайын қосыңыз, мысалы 10.10.10.105.

6. **Тұзақтар** қойындысында **Қоғамдастық атауы** өрісіне `kaspersky` енгізіңіз.

7. Өзгерістерді сақтау және қызмет сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

8. ManageEngine MIB Browser шолғышында adminkit.mib файлын Kaspersky Security Center орнату қалтасынан жүктеп алыңыз. Әдепкі бойынша, adminkit.mib файлы <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp қалтасында орналасқан.

9. ManageEngine MIB Browser шолғышы терезесінің **Құрылғы** өрісінде Kaspersky Security Center Басқару сервері орнатылған құрылғының IP мекенжайын қосыңыз.

SNMP қызметі Simple Network Management Protocol (SNMP) арқылы Басқару серверінен ақпаратты алу үшін конфигурацияланған.

SNMP агенті және нысан идентификаторлары

Kaspersky Security Center бағдарламасы үшін SNMP агенті, Басқару серверін орнату кезінде орнатушы тіркейтін `klsnmpag.dll` динамикалық кітапханасы түрінде іске асырылған. SNMP агенті `snmp.exe` процесінің ішінде жұмыс істейді (Windows қызметі болып табылады). Үшінші тарап бағдарламалары Басқару сервері өнімділігінің статистикасын алу үшін SNMP протоколын қолданады (есептегіштер түрінде ұсынылған).

Әрбір есептегіштің бірегей *нысан индентификаторы* бар (сондай-ақ, бұдан әрі OID, object identifier). Нысан идентификаторы – нүктелермен бөлінген сандар бірізділігі. Басқару сервері нысандарының идентификаторлары 1.3.6.1.4.1.23668.1093 префиксінен басталады. Есептегіш OID – осы префиксті есептегішті сипаттайтын суффикске қосу. Мысалы, OID мәні 1.3.6.1.4.1.23668.1093.1.1.4 болып табылатын есептегіш суффиксінің мәні 1.1.4.

Сіз SNMP клиентін (мысалы, Zabbix) жүйеңіздің күйін бақылау үшін қолдана аласыз. Ақпарат алу үшін, сіз OID мәнін тауып, осы мәнді өзіңіздің SNMP клиентіңізге енгізе аласыз. Содан соң, сіздің SNMP клиентіңіз сізге жүйеңіздің күйін сипаттайтын басқа мәнді қайтарады.

Есептегіштер тізімі және есептегіштер түрлері Басқару серверіндегі `adminkit.mib` файлында. *MIB* дегеніміз – Management Information Base. Сіз `.mib` файлдарын есептегіштің мәндерін сұрауға және көрсетуге арналған MIB Viewer бағдарламасы көмегімен импорттап, талдай аласыз.

Нысан идентификаторынан жол есептегіші атауын алу

Үшінші тарап бағдарламаларына ақпарат беру мақсатында нысан идентификаторын (OID) пайдалану үшін сізге осы OID идентификаторынан жол есептегішінің атын алу қажет болуы мүмкін.

OID идентификаторынан жол есептегішінің атын алу үшін:

1. Мәтіндік редакторда, Басқару серверіндегі `adminkit.mib` файлын ашыңыз.
2. Бірінші мәнді сипаттайтын атаулар кеңістігін табыңыз (солдан оңға қарай).

   Мысалы, OID 1.1.4 суффиксі үшін бұл `"counters" (::= { kladminkit 1 })` болады.
3. Екінші мәнді сипаттайтын атаулар кеңістігін табыңыз.

   Мысалы, OID 1.1.4 суффиксі үшін бұл `counters 1` болады, оның мағынасы `deployment`.
4. Үшінші мәнді сипаттайтын атаулар кеңістігін табыңыз.

   Мысалы, OID 1.1.4 суффиксі үшін бұл `deployment 4` болады, оның мағынасы `hostsWithAntivirus`.

Жол есептегіші атауы – бұл осы мәндердің біріктірілуі, мысалы, `<MIB base namespace>.counters.deployment.hostsWithAntivirus` және бұл 1.3.6.1.4.1.23668.1093.1.1.4 мәніне ие OID идентификаторына сай келеді.

SNMP үшін нысан идентификаторларының мәндері

Төмендегі кестеде үшінші тарап бағдарламаларына Басқару серверінің өнімділігі туралы ақпаратты беру үшін пайдаланылатын нысан идентификаторының (бұдан әрі - OID) мәндері мен сипаттамалары келтірілген.

SNMP үшін нысан идентификаторлары параметрлерінің мәндері мен сипаттамалары

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Орналастыру күйі. Күй келесі мәндердің біріне ие болуы мүмкін: • **Ақпараттық хабар**. Лицензия бұдан былай N құрылғылар үшін қолданылмайды. • **Ескерту**. Келесілердің бірі: Басқару сервері топтарындағы N құрылғыларда Kaspersky бағдарламалары орнатылған M құрылғылар (N > M). L лицензиясының мерзімі N құрылғыларда M күннен кейін өтіп кетеді. Бағдарламаларды орнату бойынша T тапсырмасы N құрылғыларда аяқталды, M құрылғылар үшін қайта іске қосу қажет. • **Критикалық**. Лицензия мерзімі N құрылғы үшін өтіп кеткен. • **ОК**. Жоғары аталғандардың ешқайсысы.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	deploymentStatus көрсетіп тұрғандай, Басқару серверінің топтарында басқарылатын бағдарламалар орнатылмаған құрылғылар тым көп. Басқарылатын бағдарламалары жоқ бірнеше құрылғы анықталған болса, мәні 1-ге, ал басқа жағдайда – 0-ге тең.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	deploymentStatus, кейбір құрылғыларда қашықтан орнату тапсырмасын орындау мүмкін болмағанын көрсетеді. Осы құрылғылардың санын hostsRemoteInstallFailed көмегімен алуға болады.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	deploymentStatus, лицензия мерзімі жеті күннен кейін өтіп кететін бірнеше құрылғының бар екенін көрсетеді. Осы құрылғылардың санын hostsLicenseExpiring көмегімен алуға болады.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	deploymentStatus, лицензия мерзімі өтіп кеткен бірнеше құрылғының бар екенін көрсетеді. Сіз осы құрылғылардың санын hostsLicenseExpired көмегімен біле аласыз.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Басқару серверінің топтарындағы құрылғылар саны.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Басқарылатын бағдарламалары орнатылған Басқару сервері топтарындағы құрылғылардың саны.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Қашықтан орнату тапсырмасын орындау мүмкін болмаған құрылғылардың саны.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	Жарамдылық мерзімі жақын арада, 7 күннен кем уақыттан кейін өтіп кететін лицензиялық кілт идентификаторы.
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	Жарамдылық мерзімі өтіп кеткен лицензиялық кілт идентификаторы.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Лицензия мерзімі өтіп кеткенге дейінгі күндер саны. Бұл параметр үшін, лицензия мерзімінің аяқталуына 7 күннен аз уақыт қалса, оның мерзімі аяқталды. Мерзімінің аяқталуына 7 күннен артық уақыт қалса, мән 0-ге тең болады.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Лицензия мерзімі жақында, 7 күннен кем уақыттан кейін өтіп кететін лицензиясы бар құрылғылардың саны.
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Лицензия мерзімі өтіп кеткен құрылғылар саны.
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Антивирустық дерекқорларды жаңарту күйі. Күй келесі мәндердің біріне ие болуы мүмкін: • **Ақпараттық хабар**. Басқару серверіндегі немесе құрылғылардағы антивирустық дерекқорлар бір күннен артық жаңартылмаған; бағдарлама орнатылғаннан бері бір күннен аз уақыт өтті. • **Ескерту**. Басқару серверіндегі немесе құрылғылардағы антивирустық дерекқорлар 3 күннен артық жаңартылмаған. Бұл мәнді топ сипаттарында өзгертуге болады. • **Критикалық**. Басқару серверіндегі немесе құрылғылардағы антивирустық дерекқорлар 7 күннен артық жаңартылмаған. Бұл мәнді топ сипаттарында өзгертуге болады. • **ОК**. Жоғары аталғандардың ешқайсысы.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Басқару сервері көптен бері жаңартылмады. Ұзақ болып саналатын уақыт updatesStatus күйінде көрсетіледі.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Кейбір құрылғылардың ұзақ уақыт (әдепкі бойынша **Критикалық** – 7 күн және одан да көп, **Ескерту** – 3 күн) бойы жаңартылмаған. Сіз осы құрылғылардың санын hostsNotUpdated көмегімен біле аласыз.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Басқару серверінде антивирустық дерекқорлардың соңғы рет жаңартылған күні.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Ұзақ уақыт бойы жаңартылмаған антивирустық дерекқорлары бар құрылғылардың саны (әдепкі бойынша **Критикалық** - 7 күн немесе одан көп, **Ескерту** - 3 күн). **Критикалық** жаңарту күйі бар құрылғылар болса, тек сол құрылғылар ескеріледі. Жаңарту күйін updatesStatus көмегімен алуға болады.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Нақты уақыт режимінде қорғау күйі. Келесілердің бірі: • **Ескерту**. Келесілердің бірі: Басқару серверіне кіретін құрылғыда қауіпсіздіктің бұзылғаны анықталды. Шифрлау қателеріне байланысты, кейбір құрылғылар қорғаныс күйін өзгертті. Толықтай сканерлеу көптен бері орындалмады. • **Критикалық**. Басқару серверінің топтарындағы кейбір құрылғыларда антивирустық қорғаныс жұмыс істемейді. • **ОК**. Жоғары аталғандардың ешқайсысы.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Қауіпсіздік бағдарламасы кейбір құрылғыларда жұмыс істемейді. Сіз осы құрылғылардың санын hostsAntivirusNotRunning көмегімен біле аласыз.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Нақты уақыт режимінде қорғау кейбір құрылғыларда жұмыс істемейді. Сіз осы құрылғылардың санын hostsRealtimeNotRunning көмегімен біле аласыз.
psRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.2.3	Нақты уақыттағы қорғау деңгейі Әкімші орнатқан деңгейден өзгеше құрылғылар саны
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Нысандары зарарсыздандырылмаған құрылғылар бар. Сіз осы құрылғылардың санын hostsNotCuredObject көмегімен біле аласыз.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Кейбір құрылғыларда қауіптер анықталды. Сіз осы құрылғылардың санын hostsTooManyThreats көмегімен біле аласыз.
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Жүйенің вирустың тарауы күйі. Вирустардың белгілі бір саны белгіленген уақыт ішінде анықталған болса, мәні 1-ге, ал басқа жағдайларда – 0-ге тең болады. Вирустардың саны және уақыты Басқару серверінде Вирустық шабуыл параметрі көмегімен көрсетіледі.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Осалдықтар анықталды.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Құрылғының қорғаныс күйін өзгерткен шифрлау қателері анықталды.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Кейбір құрылғыларда осалдықтар анықталды.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Ұзақ уақыт бойы толық сканерлеусіз құрылғылар анықталды.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Желілік агент қайта іске қосылғаннан кейін ғана іске қосылатын құрылғылар анықталды.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Қауіпсіздік бағдарламалары іске қосылмаған құрылғылар саны.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Нақты уақыт режимінде қорғау іске қосылмаған құрылғылар саны.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Нақты уақыт режимінде қорғау деңгейі жарамсыз болып табылатын құрылғылар саны.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Нысандары зарарсыздандырылмаған құрылғылар саны.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Қауіптері бар құрылғылар саны.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Антивирустық толықтай сканерлеу күйі келесілердің бірі: • **Ақпараттық хабар**. Бағдарламаны орнатқан сәттен бастап 7 күннен кем уақыт өтті. • **Ескерту**. Толықтай сканерлеу, бағдарлама орнатылған сәттен бастап 7 күннен артық уақыт бойы жүргізілмеді. • **Критикалық**. Толықтай сканерлеу, бағдарлама орнатылған сәттен бастап 14 күннен артық уақыт бойы жүргізілмеді. • **OK**. Жоғары аталғандардың ешқайсысы.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Тексеру белгілі бір уақыт бойы орындалмаған кейбір құрылғылар. Сіз осы құрылғылардың санын hostsNotScannedLately көмегімен біле аласыз. Уақыты fullScanStatus күйінде көрсетіледі.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Тексеру белгілі бір уақыт бойы орындалмаған құрылғылар саны. Уақыты fullScanStatus күйінде көрсетіледі.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Басқару серверінің логикалық желісінің күйі. Келесілердің бірі: • **Ескерту**. Қатынасу мүмкін емес Ескерту күйі бар құрылғылар бар болса немесе Басқару серверінің ешбір тобына жатпайтын құрылғылар бар болса. • **Критикалық**. Басқару сервері бақылай алмай жатқан құрылғылар болса немесе қатынасу мүмкін емес Критикалық күйі бар құрылғылар болса. • **OK**. Жоғары аталғандардың ешқайсысы.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Кейбір құрылғылардың ұзақ уақыт бойы Басқару серверіне қосылмаған (**Ескерту** күйі бар құрылғылар үшін 7 күн және одан да көп және **Критикалық** күйі бар құрылғылар үшін 4 күн). Сіз осы құрылғылардың санын hostsNotConnectedLongTime көмегімен біле аласыз.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Басқару сервері бақылай алмай жатқан құрылғылардың бар. Сіз осы құрылғылардың санын hostsControlLost көмегімен біле аласыз.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Басқару серверінің ешбір тобына кірмейтін Басқару сервері анықтаған құрылғылардың саны.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Басқару сервері топтарының саны.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Ұзақ уақыт бойы Басқару серверіне қосылмаған құрылғылардың саны. Ұзақ болып саналатын уақыт notConnectedLongTime күйінде көрсетіледі.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Басқару сервері бақыламайтын құрылғылардың саны.

Нысан идентификаторларының мәндері	Деректердің сандық түрі	OID	Сипаттамасы
`eventsStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.6.1	Оқиғалар ішкі жүйесінің күйі келесілердің бірі: • **Ескерту**. Келесілердің бірі: Басқару сервері топтарының құрылғылары ұзақ уақыт бойы Windows жаңартуларын іздемеді. Күймен байланысты мәселелер туындаған құрылғылар бар. • **Критикалық**. Келесілердің бірі: Кем дегенде бір құрылғыда "критикалық оқиға" бар. Кемінде бір құрылғыда "Функционалдық ақау" деңгейі бар оқиға орын алды. Кемінде бір құрылғыда тапсырманың сәтсіз аяқталуы оқиғасы бар. Басқару сервері топтарының құрылғылары ұзақ уақыт бойы Windows жаңартуларын іздемеді. Күймен байланысты мәселелер туындаған құрылғылар бар. • **Ақпараттық хабар.** Келесілердің бірі: Барлық құрылғыларда вирустарды толықтай сканерлеудің соңғы аптасынан аз уақыт өтті. Қашықтан орнату тапсырмалары аяқталды және ешбір құрылғы қайта іске қосуды қажет етпейді. Басқару серверінің соңғы жаңартуынан бері бір аптадан аз уақыт өтті. Басқару сервері ұзақ уақыт бойы жаңартылмаған, бірақ қазіргі уақытта жаңарту жүргізілуде. • **OK**. Жоғары аталғандардың ешқайсысы.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	`eventsStatus`, Басқару серверінде критикалық оқиғалардың орын алғанын көрсетеді. Сіз осы оқиғалардың санын `criticalEventsCount` көмегімен ала аласыз. Кез келген құрылғыда кемінде бір критикалық оқиға болса, мәні 1-ге, ал басқа жағдайда – 0-ге тең.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Басқару серверіндегі критикалық оқиғалардың саны.

Ақаулықтарды жою

Бұл бөлімде SNMP қызметін пайдалану кезінде кездесетін бірнеше типтік мәселелердің шешімдері келтірілген.

Үшінші тарап бағдарламасы SNMP қызметіне қосыла алмайды

SNMP қызметінің Kaspersky Security Center-мен пайдалану үшін SNMP қызметін конфигурациялау бөлімінде сипатталғандай орнатылғанын және конфигурацияланғанын тексеріңіз.

SNMP қызметі жұмыс істейді, бірақ үшінші тарап бағдарламасы ешқандай мән ала алмайды

SNMP агентін трассалауға рұқсат етіңіз және бос емес файл жасалғанына көз жеткізіңіз. Бұл SNMP агенті дұрыс тіркелгенін және жұмыс істеп тұрғанын білдіреді. Осыдан кейін, қызмет параметрлерінде SNMP қызметінен қосылуға рұқсат етіңіз. Қызмет SNMP агентімен бір құрылғыда жұмыс істеп тұрса, IP мекенжайлары тізімінде осы құрылғының IP мекенжайы немесе `loopback 127.0.0.1` болуы мүмкін.

Windows жүйесінде агенттермен өзара әрекеттесетін SNMP қызметі болуы керек. regedit көмегімен Windows тізімдемесінде SNMP агенттеріне апаратын жолдарды көрсетуге болады.

- Windows 10 үшін:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Windows Vista және Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Сондай-ақ, regedit көмегімен SNMP агентін трассалауға рұқсат бере аласыз.

- 32 разрядты жүйе үшін:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- 64 разрядты жүйе үшін:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

Мәндер Басқару консолінің күйлеріне сай келмейді

Басқару серверіне түсетін жүктемені азайту мақсатында, SNMP агенті үшін мәндерді кэштеу жүзеге асырылған. Кэшті өзектендіру мен Басқару сервердегі өзгертілетін мәндер арасындағы кідіріс SNMP агенті қайтаратын мәндер мен нақты мәндер арасындағы сәйкессіздікті тудыруы мүмкін. Үшінші тарап бағдарламаларымен жұмыс істеу кезінде ықтимал кідірісті ескеру қажет.

Бұлтты ортада жұмыс істеу

Бұл бөлімде Amazon Web Services, Microsoft Azure және Google Cloud сияқты бұлтты ортада Kaspersky Security Center-ді орналастыру және қызмет көрсету туралы ақпарат келтірілген.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Бұлтты ортада жұмыс істеу туралы

Kaspersky Security Center 15.1 бағдарламасы физикалық құрылғылармен жұмыс істеп қана қоймай, бұлтты ортада жұмыс істеу үшін мүмкіндіктер ұсынады. Kaspersky Security Center бағдарламасы келесі виртуалды машиналармен жұмыс істейді:

- Amazon EC2 даналары (бұдан әрі *даналар* деп те аталады). Amazon EC2 данасы – бұл Amazon Web Services (AWS) платформасы негізінде жасалған виртуалды машина. Kaspersky Security Center бағдарламасы AWS *API* (Application Programming Interface, қолданбаның бағдарламалық интерфейсі) қолданады.
- Microsoft Azure виртуалды машиналары. Kaspersky Security Center бағдарламасы API Azure қолданады.
- Google Cloud виртуалды машиналарының даналары. Kaspersky Security Center бағдарламасы API Google қолданады.

Сіз Kaspersky Security Center бағдарламасын данада немесе виртуалды машинада бұлтты ортадағы құрылғылардың қорғанысын басқару үшін орналастыра аласыз және бұлтты ортада жұмыс істеу үшін Kaspersky Security Center бағдарламасының арнайы мүмкіндіктерін пайдалана аласыз. Бұл мүмкіндіктер келесіні қамтиды:

- бұлтты ортадағы даналар API көмегімен сауалнама жүргізу;
- бұлтты ортадағы құрылғыларда Желілік агент пен қауіпсіздік бағдарламаларын орнату үшін API құралдарын пайдалану;
- белгілі бір бұлттық сегментке жататын құрылғыларды іздеу.

Сондай-ақ, физикалық құрылғыларды қорғау үшін Kaspersky Security Center Басқару сервері орналастырылған дананы немесе виртуалды машинаны пайдалануға болады (мысалы, мұндай бұлтты сервер физикалық серверге қарағанда техникалық қызмет көрсету мен күтіп ұстауда тиімдірек болса). Бұл жағдайда, Басқару серверімен атқарылатын жұмыс, физикалық құрылғыға орнатылған Басқару серверіндей жүзеге асырылатын болады.

Ақылы Amazon Machine Image (AMI) арқылы (AWS-те) орналастырылған немесе қызмет көлеміне байланысты ай сайынғы тарифтік жазылым негізінде (Azure-де) пайдаланылатын Kaspersky Security Center бағдарламасында Осалдықтар мен патчтарды басқару мүмкіндіктері автоматты түрде іске қосылады, бірақ Ұялы құрылғыларды басқаруды белсендіру мүмкін емес.

Басқару сервері Басқару консолімен бірге орнатылады. Kaspersky Security for Windows Server сервері де Басқару сервері орнатылған құрылғыға автоматты түрде орнатылады.

Бұлтты ортада жұмыс істеу ерекшеліктерін ескере отырып, Kaspersky Security Center бағдарламасын бұлтты ортаны конфигурациялау шебері арқылы конфигурациялауға болады.

Сценарий: Бұлтты ортада орналастыру

Бұл бөлімде Amazon Web Services, Microsoft Azure және Google Cloud сияқты бұлтты ортада жұмыс істеуге арналған Kaspersky Security Center орналастыру сценарийі сипатталған.

Орналастыру сценарийі аяқталғаннан кейін, Kaspersky Security Center Басқару сервері және Басқару консолі әдепкі бойынша параметрлермен іске қосылып, конфигурацияланады. Таңдалған Amazon EC2 даналарында немесе Microsoft Azure виртуалды машиналарында Kaspersky Security Center басқаратын антивирустық қорғаныс орналастырылады. Алдағыда, сіз Kaspersky Security Center бағдарламасын толығырақ конфигурациялай аласыз, басқару топтарының күрделі құрылымын жасай аласыз, топтар үшін әртүрлі саясат пен тапсырмалар жасай аласыз.

Бұлтты ортада жұмыс істеу үшін Kaspersky Security Center орналастыру келесі қадамдардан тұрады:

1. Дайындық.
2. Басқару серверін орналастыру.
3. Kaspersky антивирустық бағдарламаларын қорғалуы қажетті виртуалды құрылғыларға орнату.
4. Жаңартуларды жүктеу параметрлерді конфигурациялау.
5. Құрылғыны қорғау күйі туралы есептермен жұмыс істеу параметрлерін конфигурациялау.

Бастапқы конфигурациялау үшін бұлтты ортаны конфигурациялау шебері бар. Шебер Kaspersky Security Center бағдарламасын дайын кескіннен алғаш рет орналастыру кезінде автоматты түрде іске қосылады. Сіз шеберді кез келген сәтте іске қоса аласыз. Сондай-ақ, сіз шебер орындайтын барлық іс-әрекеттерді өз бетінше орындай аласыз.

Kaspersky Security Center Басқару серверін бұлтты ортада орналастыруға кемінде бір сағат, ал бұлтты ортада қорғанысты орналастыруға жалпы алғанда – кемінде бір жұмыс күнін жұмсау ұсынылады.

Kaspersky Security Center бағдарламасын бұлтты ортада орналастыру келесі кезеңдерден тұрады:

1. **Бұлттық сегменттердің конфигурациясын жоспарлау**

   Kaspersky Security Center бағдарламасының бұлтты ортадағы жұмысын танысыңыз. Басқару сервері қайда орналастырылатынын жоспарлаңыз (бұлтты орта ішінде немесе одан тыс жерде); қанша бұлттық сегментті қорғағыңыз келетінін анықтаңыз. Басқару серверін бұлтты ортадан тыс орналастыруды жоспарласаңыз немесе 5000-нан астам құрылғыны қорғауды жоспарласаңыз, онда сізге Басқару серверін қолмен орнату қажет болады.

   Google Cloud бұлтты ортасымен жұмыс істеу үшін Басқару серверін қолмен орнатуға болады.

2. **Ресурстарды жоспарлау**

   Орналастыру үшін қажетті барлық шарттардың орындалғанына көз жеткізіңіз.

3. **Дайын кескін түріндегі Kaspersky Security Center бағдарламасына жазылу**

   AWS Marketplace дүкенінен дайын AMI кескіндерінің бірін таңдаңыз немесе Azure Marketplace дүкенінде SKU пайдалану үшін ай сайынғы шоттарды пайдалануды таңдаңыз, қажет болса дүкен ережелеріне сәйкес төлеңіз (немесе BYOL моделін пайдаланыңыз) және Amazon EC2 данасын немесе Kaspersky Security Center бағдарламасы орнатылған Microsoft Azure виртуалды машинасын орналастыру үшін кескінді пайдаланыңыз.

   Бұл кезең, Басқару серверін данаға немесе виртуалды машинаға бұлтты ортада орналастыруды жоспарласаңыз және бұл арада, 5000-нан аспайтын құрылғыны қорғауды жоспарласаңыз ғана қажет. Әйтпесе, бұл кезең керек емес және оның орнына Басқару серверін, Басқару консолін және ДҚБЖ қолмен орнату қажет.

   Бұл қадам Google Cloud үшін қолжетімді емес.

4. **ДҚБЖ орналасқан жерін анықтау**

   ДҚБЖ орналасатын жерін анықтау.

Дерекқорды бұлтты ортадан тыс жерде қолдануды жоспарласаңыз, онда сізде жұмысқа жарамды дерекқордың бар екеніне көз жеткізіп алыңыз.

Amazon Relational Database Service (RDS) қызметін қолдануды жоспарлап жатсаңыз, онда AWS бұлтты ортасында RDS дерекқорын жасаңыз.

Microsoft Azure SQL ДҚБЖ қолдануды жоспарлап жатсаңыз, онда Microsoft Azure бұлтты ортасында Azure дерекқоры қызметі бар дерекқорды жасаңыз.

Google MySQL қолдануды жоспарлап жатсаңыз, онда Google Cloud бұлтты ортасында дерекқорды жасаңыз (толық ақпаратты https://cloud.google.com/sql/docs/mysql құжаттамасынан қараңыз).

5. **Таңдалған құрылғыларға Басқару сервері мен Басқару консолін (Microsoft Management Console негізінде және/немесе веб-интерфейс негізіндегі Консоль негізінде) қолмен орнату**

   Басқару серверін, Басқару консолін және ДҚБЖ жүйесін таңдалған құрылғыларға Kaspersky Security Center орнату негізгі сценарийінде сипатталғандай орнатыңыз.

   Бұл кезең, Басқару серверін бұлтты ортадан тыс жерде орналастыруды жоспарлап жатсаңыз немесе қорғанысты 5000-нан астам құрылғыға орналастыруды жоспарлап жатсаңыз керек. Содан соң, сіздің Басқару серверіңіз жабдыққа қойылатын талаптарға сай келетіндігіне көз жеткізіңіз. Әйтпесе, бұл кезең қажет емес және AWS Marketplace дүкенінде, Azure Marketplace дүкенінде немесе Google Cloud дүкенінде Kaspersky Security Center бағдарламасына дайын кескін түрінде жазылу жеткілікті.

6. **API бұлттық қызметтері бар Басқару серверінің жұмыс істеуі үшін құқықтарды қамтамасыз ету.**

   AWS сервисінде AWS басқару консоліне өтіп, IAM рөлін немесе IAM пайдаланушысының есептік жазбасын жасаңыз. Жасалған IAM рөлі (немесе IAM пайдаланушысының есептік жазбасы) Kaspersky Security Center бағдарламасына AWS API интерфейсімен жұмыс істеуге: бұлттық сегменттерде сауалнама өткізуге және қорғанысты орналастыруға мүмкіндік береді.

   Azure қызметінде құпиясөзі бар қолданбаның идентификаторы мен жазылымын жасаңыз Kaspersky Security Center бағдарламасы осы есептік деректерді Azure API интерфейсінде жұмыс істеу: бұлттық сегменттерде сауалнама өткізу және қорғанысты орналастыру үшін қолданады.

   Google Cloud бұлтты ортасында жобаны тіркеңіз, жоба идентификаторын және жеке кілтті алыңыз. Kaspersky Security Center бағдарламасы осы есептік деректерді Google API көмегімен бұлттық сегменттерде сауалнама өткізу үшін қолданады.

7. **Қорғалатын даналар үшін IAM рөлін жасау (тек AWS үшін)**

   AWS басқару консолінде AWS сервистеріне сұраулар салу үшін рұқсаттар жиынтығын анықтайтын IAM рөлін жасаңыз. Кейінірек, жасалған рөлді жаңа даналарға тағайындайтын боласыз. IAM рөлі бағдарламаларды Kaspersky Security Center бағдарламасы көмегімен даналарға орнату үшін керек.

8. **Дерекқорды Amazon Relational Database Service немесе Microsoft Azure SQL көмегімен дайындау**

   Amazon Relational Database Service (RDS) дерекқорын қолдануды жоспарлап жатсаңыз, Amazon RDS дерекқоры данасын және дерекқордың сақтық көшірмесі сақталатын S3 орнын жасаңыз. Басқару сервері орнатылған EC2 данасында дерекқор қажет болса немесе дерекқорыңыздың басқа жерде болуын қаласаңыз, осы кезеңді өткізіп жібере аласыз.

   Microsoft Azure SQL қолдануды жоспарлап жатсаңыз, Microsoft Azure бұлтты ортасында дерекқорды және қойманың есептік жазбасын жасаңыз.

   Google MySQL қолдануды жоспарлап жатсаңыз, онда Google Cloud бұлтты ортасында дерекқорды жасаңыз (толық ақпаратты https://cloud.google.com/sql/docs/mysql құжаттамасынан қараңыз).

9. **Бұлтты ортада жұмыс істеу үшін Kaspersky Security Center лицензиялау**

   Бұлтты ортада Kaspersky Security Center жұмыс істеуі үшін лицензияңыздың бар екеніне көз жеткізіңіз және бағдарлама лицензиялар қоймасына қосуы үшін белсендіру кодын немесе кілт файлын ұсыныңыз. Бұл қадамды бұлттық ортаны конфигурациялау кезінде аяқтауға болады.

BYOL моделі бойынша тегін AMI дайын кескінінен орнатылған Kaspersky Security Center қолдансаңыз немесе Kaspersky Security Center бағдарламасын AMI кескіндерінсіз, өз бетінше орнатып жатсаңыз, бұл кезең міндетті. Осы жағдайлардың әрқайсысында, Kaspersky Security Center бағдарламасын белсендіру үшін сізге Kaspersky Security for Virtualization бағдарламасына немесе Kaspersky Hybrid Cloud Security бағдарламасына лицензия керек.

Дайын кескіннен орнатылған Kaspersky Security Center бағдарламасын қолдансаңыз, онда бұл кезең міндетті емес және бұлтты ортаны конфигурациялау шеберінің тиісті терезесі көрсетілмейді.

10. **Бұлтты ортадағы түпнұсқалық растама**

Kaspersky Security Center бағдарламасы қажетті рұқсаттармен жұмыс істей алуы үшін Kaspersky Security Center бағдарламасында AWS, Azure немесе Google Cloud есептік деректеріңізді көрсетіңіз. Бұл кезең бұлтты ортада авторизациямен аяқталуы мүмкін.

11. **Басқару серверінің бұлттық сегментте сауалнама өткізуі арқылы бұлттық сегменттегі құрылғылар туралы мәліметтерді алуы.**

Бұлттық сегменттерде сауалнама өткізуді бастаңыз. AWS бұлтты ортасында Kaspersky Security Center бағдарламасы, IAM рөлінің құқықтары немесе IAM пайдаланушысы құқықтары қамтамасыз ететін қатынасу мүмкіндігіне ие барлық даналардың мекенжайлары мен аттарын алады. Microsoft Azure бұлтты ортасында, Kaspersky Security Center бағдарламасы Оқырман рөлінің құқықтары қамтамасыз ететін қатынасу мүмкіндігіне ие барлық виртуалды машиналардың мекенжайлары мен аттарын алады.

Алдағыда, Kaspersky Security Center көмегімен табылған даналарға немесе виртуалды машиналарға Kaspersky және басқа өндірушілердің бағдарламаларын орната аласыз.

Kaspersky Security Center бағдарламасы сауалнама үнемі іске қосып тұрады, жаңа даналар немесе виртуалды машиналар пайда болса, олар автоматты түрде анықталады.

12. **Желінің барлық құрылғыларын Cloud басқару тобына біріктіру**

Барлық анықталған даналарды немесе виртуалды машиналарды **Басқарылатын құрылғылар\Cloud** басқару тобына жылжытыңыз, осылайша олар орталықтан басқару үшін қолжетімді болады. Құрылғыларды ішкі топтарға бөлгіңіз келсе, мысалы, оларға қандай операциялық жүйенің орнатылғанына қарай, сіз **Басқарылатын құрылғылар\Cloud** тобының ішінде бірнеше басқару тобын жасай аласыз. Үнемі сауалнама өткізу кезінде анықталатын барлық құрылғыларды Басқарылатын құрылғылар**Cloud** тобына **автоматты түрде жылжытуды конфигурациялай** аласыз.

13. **Желідегі құрылғыларды Желілік агент арқылы Басқару серверімен байланыстыру**

Желілік агентті бұлтты ортадағы құрылғыларға орнатыңыз. Kaspersky Security Center құрамдасы құрылғының Басқару серверімен байланысуын қамтамасыз етеді. Желілік агенттің параметрлері әдепкі бойынша автоматты түрде конфигурацияланады.

Желілік агентті әрбір құрылғыға жергілікті түрде орната аласыз. Сондай-ақ, Желілік агентті құрылғыларға қашықтан, Kaspersky Security Center бағдарламасы көмегімен орната аласыз. Немесе сіз осы кезеңді өткізіп жіберіп, қауіпсіздік бағдарламаларының соңғы нұсқаларымен бірге Желілік агентті орната аласыз.

14. **Қауіпсіздік бағдарламаларының соңғы нұсқаларын желідегі құрылғыларға орнату**

Қауіпсіздік бағдарламаларын орнатқыңыз келетін құрылғыларды таңдап, осы құрылғыларға қауіпсіздік бағдарламаларының соңғы нұсқаларын орнатыңыз. Орнатуды қашықтан, Басқару серверіндегі Kaspersky Security Center көмегімен немесе жергілікті түрде жүзеге асыра аласыз.

Бәлкім, сізге осы бағдарламалар үшін орнату пакеттерін қолмен жасауға тура келетін де шығар.

Linux басқаратын виртуалды машиналар мен даналар үшін Kaspersky Endpoint Security for Linux бағдарламасы бар.

Windows басқаратын виртуалды машиналар мен даналар үшін Kaspersky Security for Windows Server бағдарламасы бар.

15. **Жаңартуды конфигурациялау**

Бұлтты ортаны конфигурациялауды бастағанда **Осалдықтарды және қажетті жаңартуларды іздеу** тапсырмасы автоматты түрде жасалады. Сіз оны қолмен де жасай аласыз. Бұл тапсырма бағдарламалардың қажетті жаңартуларын автоматты түрде іздеуді және жүктеуді, содан соң Kaspersky Security Center құралдарымен желідегі құрылғыларға орнатуды қамтамасыз етеді.

Бұлтты ортаны конфигурациялауды аяқтағаннан кейін, келесі қадамды орындау ұсынылады:

1. **Есептермен жұмысты конфигурациялау**

   Сіз есептерді **Басқару сервері** түйінінің жұмыс аймағындағы **Мониторинг** қойыншасында қарай аласыз. Сіз есептерді электрондық пошта арқылы да ала аласыз. **Мониторинг** қойыншасындағы есептер әдепкі бойынша қолжетімді. Есептерді электрондық пошта арқылы алуды конфигурациялау үшін, есептер жіберілетін электрондық пошта мекенжайларын көрсетіп, есептердің пішімін конфигурациялаңыз.

Нәтижелер

Сценарий аяқталғаннан кейін, жылдам іске қосудың сәтті орындалғанына көз жеткізе аласыз:

- Басқару серверіне Басқару консолінің көмегімен немесе Kaspersky Security Center Web Console көмегімен қосыла аласыз.
- Басқарылатын құрылғыларда Kaspersky қауіпсіздік бағдарламаларының соңғы нұсқалары орнатылып, жұмыс істеуде.
- Kaspersky Security Center бағдарламасы барлық басқарылатын құрылғылар үшін әдепкі бойынша саясаттар мен тапсырмаларды жасады.

Kaspersky Security Center бағдарламасын бұлтты ортада орналастырудың алғышарттары

Kaspersky Security Center бағдарламасын Amazon Web Services немесе Microsoft Azure сияқты бұлтты ортада орналастыруды бастамас бұрын, сізде келесілердің бар екеніне көз жеткізіңіз:

- Интернетке қатынас
- Келесі есептік жазбалардың бірі:
  - Amazon Web Services есептік жазбасы (AWS-пен жұмыс істеу үшін)
  - Microsoft есептік жазбасы (Azure-мен жұмыс істеу үшін)
  - Google есептік жазбасы (Google Cloud-пен жұмыс істеу үшін)
- Келесілердің бірі:
  - Kaspersky Security for Virtualization лицензиясы
  - Kaspersky Hybrid Cloud Security лицензиясы

- Осындай лицензияны (Kaspersky Security for Virtualization немесе Kaspersky Hybrid Cloud Security) сатып алуға арналған қаражат
- Azure Marketplace дүкенінде дайын кескінге ақы төлеуге арналған қаражат

- Kaspersky Endpoint Security for Linux және Kaspersky Security for Windows Server бағдарламаларының соңғы нұсқаларына арналған нұсқаулықтар

Бұлтты ортадағы Басқару серверіне қойылатын аппараттық талаптар

Бұлтты ортада орналастыру үшін Басқару сервері мен дерекқор серверіне қойылатын талаптар физикалық Басқару серверімен бірдей (қанша құрылғыны басқарғыңыз келетініне байланысты). Кеңейтілген ақпаратты бұлтты ортаға арналған құжаттамадан қараңыз.

Бұлтты ортада лицензиялау нұсқалары

Бұлтты ортадағы жұмыс Kaspersky Security Center базалық функционалдығына кірмейді және лицензияны талап етпейді.

Kaspersky Security Center бағдарламасы бұлтты ортада жұмыс істеу үшін лицензиялаудың екі нұсқасын ұсынады:

- Ақылы AMI кескіні (Amazon Web Services қызметі) немесе SKU пайдалану үшін ай сайынғы шоттарды пайдалану (Microsoft Azure қызметі).

  Kaspersky Security Center лицензиялаудың бұл нұсқасы Kaspersky Endpoint Security for Linux және Kaspersky Security for Windows Server үшін лицензияны да ұсынады. Сіз бұлтты ортаның ережелеріне сәйкес төлеуіңіз керек.

  Бұл модель бір Басқару сервері үшін ең көбі 200 клиент құрылғысын басқаруға мүмкіндік береді.

- BYOL (Bring Your Own License) моделі бойынша өз лицензияңыз қолданылған дайын тегін кескін.

  AWS немесе Azure қызметінде Kaspersky Security Center лицензиялау үшін бағдарламалардың бірін пайдалануға лицензия қажет:

  - Kaspersky Security for Virtualization;
  - Kaspersky Hybrid Cloud Security.

  Бұл модель бір Басқару сервері үшін 100 000-ға дейін клиент құрылғысын басқаруға мүмкіндік береді. Бұл модель AWS, Azure немесе Google бұлтты ортасынан тыс құрылғыларды басқаруға да мүмкіндік береді.

  Сіз BYOL моделін келесі жағдайлардың кез келгенінде таңдай аласыз:

  - Kaspersky Security for Virtualization үшін қолданыстағы лицензияңыз бар болса;
  - Kaspersky Hybrid Cloud Security үшін қолданыстағы лицензияңыз болса;
  - Kaspersky Security Center орналастырудың дәл алдында лицензияны сатып алғыңыз келсе.

Kaspersky Security Center [бастапқы конфигурациялау кезеңінде](#) сізден белсендіру кодын немесе кілт файлын сұрайды.

BYOL таңдау кезінде, сізге Kaspersky Security Center бағдарламасын қолдану үшін Azure Marketplace немесе AWS Marketplace дүкені арқылы ақы төлеудің қажеті жоқ.

Екі жағдайда да Осалдықтар мен патчтарды басқару мүмкіндіктері автоматты түрде белсендіріледі, бірақ Ұялы құрылғыларды басқару мүмкіндігін белсендіру мүмкін емес.

Kaspersky Hybrid Cloud Security лицензиясын қолдана отырып, бұлтты ортаны қолдау функциясын белсендіруге әрекеттенген кезде, қате пайда болса, кілт файлын пайдаланыңыз.

Kaspersky Security Center бағдарламасына жазылғаннан кейін, сіз Amazon Elastic Compute Cloud (Amazon EC2) немесе Kaspersky Security Center Басқару сервері бар Microsoft Azure виртуалды машинасын аласыз. Kaspersky Security for Windows Server және Kaspersky Endpoint Security for Linux орнату пакеттері Басқару серверінде қолжетімді. Бұл бағдарламаларды бұлтты ортадағы құрылғыларға орнатуға болады. Осы бағдарламаларды лицензия бойынша белсендіру қажет емес.

Егер басқарылатын құрылғы Басқару сервері желісінде бір аптадан артық көрінбесе, осы құрылғыдағы қауіпсіздік бағдарламасы (Kaspersky Security for Windows Server немесе Kaspersky Endpoint Security for Linux) шектеулі функционалдылық режиміне өтеді. Бағдарламаны қайта белсендіру үшін қауіпсіздік бағдарламасы орнатылған құрылғыны Басқару сервері желісінде қайтадан көрінетіндей етіп жасау қажет.

Бұлтты ортада жұмыс істеуге арналған дерекқор параметрлері

Сізде Kaspersky Security Center-мен жұмыс істеу үшін дерекқор болуы керек. Kaspersky Security Center бағдарламасын AWS, Microsoft Azure немесе Google Cloud ортасына орналастырған кезде сізде үш параметр бар:

- Басқару сервері бар бір құрылғыда жергілікті дерекқорды жасаңыз. Kaspersky Security Center 5000-ға дейін басқарылатын құрылғыға қолдау көрсете алатын SQL Server Express дерекқорымен бірге жеткізіледі. SQL Server Express шығарылымы қажеттіліктеріңіз үшін жеткілікті болса, осы опцияны таңдаңыз.

- AWS бұлтты ортасында Relational Database Service (RDS) немесе [Microsoft Azure бұлтты ортасында](#) Azure дерекқор қызметімен дерекқор жасаңыз. Егер сіз SQL Express-тен ерекшеленетін ДҚБЖ қолданғыңыз келсе, осы параметрді таңдаңыз. Сіздің деректеріңіз бұлтты ортада көшіріліп, сонда олар қалады және сізде қосымша шығындар болмайды. Егер сіз Kaspersky Security Center-мен жергілікті жерде жұмыс істеп жатсаңыз және дерекқорыңызда кейбір деректер болса, деректеріңізді жаңа дерекқорға тасымалдауға болады.

  Google Cloud платформасында жұмыс істеу мақсатында тек MySQL үшін Cloud SQL пайдалануға болады.

- Қолданыстағы дерекқор серверін пайдаланыңыз. Егер сіз дерекқор серверін пайдаланып жатсаңыз және оны Kaspersky Security Center үшін пайдаланғыңыз келсе, осы параметрді таңдаңыз. Егер бұл сервер бұлтты ортадан тыс жерде орналасса, сіздің деректеріңіз интернет арқылы көшіріліп, бұл қосымша шығындарға әкелуі мүмкін.

Kaspersky Security Center бағдарламасын бұлтты ортада орналастыру процедурасында дерекқор құруға (таңдауға) арналған нақты қадамдар бар.

Amazon Web Services бұлтты ортасындағы жұмыс

Бұл бөлімде, Amazon Web Services-те Kaspersky Security Center-мен жұмыс істеуге қалай дайындалу керектігі сипатталған.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Amazon Web Services бұлтты ортасындағы жұмыс туралы

Сіз Kaspersky Security Center бағдарламасын AWS Marketplace қолданбалар дүкенінде AMI (Amazon Machine Image) кескіні – алдын ала конфигурацияланған виртуалды машинаның дайын кескіні түрінде сатып ала аласыз. Сіз ақылы дайын AMI немесе BYOL AMI кескініне жазыла аласыз және осы кескіннің негізінде Kaspersky Security Center Басқару сервері орнатылған Amazon EC2 данасын жасай аласыз.

AWS платформасымен жұмыс істеу үшін, атап айтқанда AWS Marketplace дүкенінен қолданбаларды сатып алу және даналар жасау үшін сізге Amazon Web Services есептік жазбасы қажет. Сіз https://aws.amazon.com/ru сайында тегін есептік жазба жасай аласыз. Сондай-ақ, қолданыстағы Amazon есептік жазбасын қолдана аласыз.

AWS Marketplace қолданбалар дүкенінде қолжетімді AMI кескініне жазылсаңыз, онда жұмысқа дайын Kaspersky Security Center бағдарламасы бар данаға ие боласыз. Бағдарламаны өзіңіз орнатудың қажеті жоқ. Бұл жағдайда, Kaspersky Security Center Басқару сервері данаға сіздің қатысуыңызсыз орнатылады. Орнатқаннан кейін, сіз Басқару консолін іске қосып, Kaspersky Security Center бағдарламасымен жұмысты бастау үшін Басқару серверіне қосыла аласыз.

AMI кескіндері не екені және AWS Marketplace қолданбалар дүкені қалай жұмыс істейтіні туралы ақпарат AWS Marketplace анықтама бетінде келтірілген. AWS платформасымен жұмыс істеу туралы, даналарды қолдану туралы және олармен байланысты түсініктер туралы ақпарат Amazon Web Services құжаттамасында көрсетілген.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Amazon EC2 данасы үшін IAM рөлі мен IAM пайдаланушысы есептік жазбаларын жасау

Бұл бөлімде Басқару серверінің дұрыс жұмыс істеуін қамтамасыз ету үшін қандай әрекеттерді орындау керектігі сипатталған. Бұл әрекеттер AWS сервистерімен, IAM рөлдерімен (Identity and Access Management) және пайдаланушы есептік жазбаларымен жұмыс істеуді қамтиды. Сондай-ақ, клиент құрылғыларына Желілік агентті, содан кейін Kaspersky Security for Windows Server және Kaspersky Endpoint Security for Linux қорғаныс бағдарламаларын орнату үшін клиент құрылғыларымен қандай әрекеттер орындалуы керектігі сипатталған.

AWS көмегімен Kaspersky Security Center Басқару серверінің жұмыс істеу құқықтарын қамтамасыз ету

Amazon Web Services бұлтты ортасындағы жұмыс стандарттары, AWS қызметтерімен жұмыс істеу үшін Басқару сервері данасына арнайы IAM рөлін тағайындауды ұсынады. AWS консолінде AWS сервистеріне сұраулар салу үшін рұқсаттар жиынтығын анықтайтын IAM рөлін жасаңыз. IAM рөлі бұлттық сегменттерде сауалнама жүргізу және даналарға бағдарламаларды орнату құқығын қамтамасыз етеді.

IAM рөлін жасап, оны Басқару серверіне тағайындағаннан кейін, сіз осы рөлді пайдаланып және Kaspersky Security Center-ге қосымша ақпарат бермей, даналардың қорғанысын орналастыра аласыз.

Алайда, келесі жағдайларда Басқару сервері үшін IAM рөлін жасаудан бас тарту орынды болуы мүмкін:

- Егер сіз қорғанысын басқаруды жоспарлап отырған құрылғылар Amazon Web Services бұлтты ортасындағы EC2 даналары болса, ал Басқару сервері одан тыс болса.
- Егер сіз бұлттық сегментте ғана емес, AWS-тегі басқа есептік жазбада жасалған басқа бұлттық сегменттерде де даналардың қорғанысын басқаруды жоспарласаңыз. Бұл жағдайда, сізге бұлттық сегментіңізді қорғау үшін IAM рөлі қажет болады. Басқа бұлттық сегментті қорғау үшін сізге IAM рөлі қажет емес.

Бұл жағдайларда сізге IAM рөлін емес, Kaspersky Security Center бағдарламасы *AWS сервистерімен жұмыс істейтін IAM пайдаланушысының есептік жазбасын* жасау керек болады. Басқару серверімен жұмысты жасамас бұрын, *AWS IAM қатынас кілті* (сондай-ақ, бұдан әрі *IAM қатынас кілті*) бар IAM пайдаланушы есептік жазбасын жасаңыз.

IAM рөлін немесе IAM пайдаланушысын жасау үшін AWS басқару консолі керек. AWS басқару консолімен жұмыс істеу үшін, сізге AWS есептік жазбасының пайдаланушы аты мен құпиясөзі керек.

Басқару сервері үшін IAM рөлін жасау

Басқару серверін орналастыру алдында, AWS басқару консолінде даналарға бағдарламаларды орнату үшін қажетті құқықтары бар IAM рөлін жасаңыз. Толығырақ AWS анықтамасында, IAM рөлдері туралы бөлімдерде.

Басқару серверіне арналған IAM рөлін жасау үшін:

1. AWS басқару консолі тармағын ашып, өзіңіздің AWS есептік жазбаңызбен кіріңіз.
2. **Рөлдер** бөлімінде келесі құқықтары бар рөл жасаңыз:
   - **AmazonEC2ReadOnlyAccess** – егер сіз тек бұлттық сегменттерде сауалнама өткізуді жоспарласаңыз және AWS API көмегімен EC2 даналарына бағдарламалар орнатуды жоспарламасаңыз.
   - **AmazonEC2ReadOnlyAccess** және **AmazonSSMFullAccess** – егер сіз бұлттық сегменттерде сауалнама өткізуді де, AWS API көмегімен EC2 даналарына бағдарламалар орнатуды да жоспарласаңыз. Бұл жағдайда, сізге EC2 қорғалатын даналарына AmazonEC2RoleforSSM құқықтары бар IAM рөлін тағайындау қажет болады.

Сізге бұл рөлді Басқару сервері ретінде пайдаланатын EC2 данасына тағайындау қажет болады.

Жасалған рөл Басқару серверіндегі барлық бағдарламалар үшін қолжетімді. Сондықтан, Басқару серверінде жұмыс істейтін кез келген бағдарлама бұлттық сегменттерде сауалнама өткізе алады немесе бұлттық сегменттегі EC2 даналарына бағдарламаларды орната алады.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Kaspersky Security Center жұмысы үшін IAM пайдаланушысы есептік жазбасын жасау

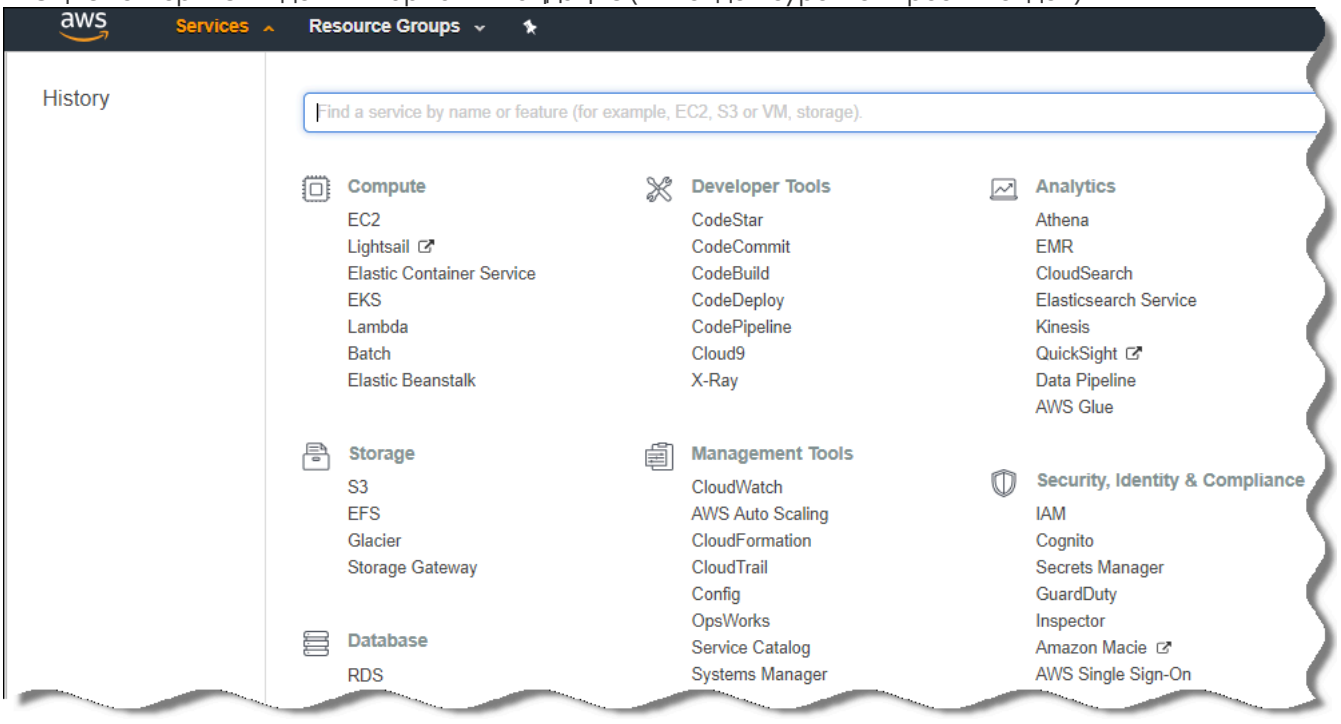
Басқару серверіне құрылғыларды табу және бағдарламаларды даналарға орнату құқығымен IAM рөлі тағайындалмаса, IAM пайдаланушысы есептік жазбасы Kaspersky Security Center-мен жұмыс істеу үшін қажет. S3 себетін пайдалансаңыз, Басқару сервері деректерінің тапсырмасын сақтық көшірмелеу үшін де дәл осы есептік жазба немесе басқа есептік жазба қажет. Қажетті құқықтары бар бір IAM пайдаланушысының есептік жазбасын немесе екі түрлі есептік жазбаны жасауға болады.

IAM пайдаланушысы үшін *IAM қатынас кілті* автоматты түрде жасалады, оны бастапқы конфигурациялау кезеңінде Kaspersky Security Center-ге ұсыну керек. IAM қатынас кілті, қатынас кілтінің идентификаторы мен құпия кілттен тұрады. IAM сервисі туралы қосымша ақпарат алу үшін келесі AWS анықтамалық беттерін қараңыз:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html;
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Қажетті құқықтары бар IAM пайдаланушысының есептік жазбасын жасау үшін:

1. AWS басқару консолін ашып, өзіңіздің есептік жазбаңызбен кіріңіз.
2. AWS қызметтері тізімінде **IAM** тармағын таңдаңыз (төмендегі суретте көрсетілгендей).



AWS басқару консолінде қызметтер тізімі

Пайдаланушы аттары тізімі мен құралмен жұмыс істеуге болатын мәзірі бар терезе ашылады.

3. Пайдаланушы есептік жазбаларын пайдаланатын консоль аймақтарына өтіп, жаңа пайдаланушы атын немесе аттарын қосыңыз.

4. Сіз қосқан пайдаланушылар үшін келесі AWS параметрлерін көрсетіңіз:

   - Қатынас түрі: **Programmatic Access**.
   - Кеңейтім шекаралары орнатылмаған.
   - Рұқсаттар:
     - **ReadOnlyAccess** – егер сіз тек бұлттық сегменттерде сауалнама өткізуді жоспарласаңыз және AWS API көмегімен EC2 даналарына бағдарламалар орнатуды жоспарламасаңыз;
     - **ReadOnlyAccess** және **AmazonSSMFullAccess** – егер сіз бұлттық сегменттерде сауалнама өткізуді де, AWS API көмегімен EC2 даналарына бағдарламалар орнатуды да жоспарласаңыз. Бұл жағдайда, EC2 қорғалған даналарына AmazonEC2RoleforSSM құқықтарымен бірге IAM рөлін тағайындауыңыз қажет.

   Рұқсаттарды қосқаннан кейін, оларды мұқият қарап шығыңыз. Параметрлерді таңдау қатесі болған жағдайда, алдыңғы экранға өтіп, параметрлерді қайтадан таңдаңыз.

5. Есептік жазбаны жасағаннан кейін жаңа IAM пайдаланушысының IAM қатынас кілті бар кесте көрсетіледі. Қатынас кілтінің идентификаторы **Access key ID** бағанында көрсетіледі. Құпия кілт **Secret access key** бағанында жұлдызшалар түрінде көрсетіледі. Құпия кілтті көру үшін **Show** түймесін басыңыз.

Жасалған есептік жазба AWS есептік жазбаңызға сәйкес келетін IAM пайдаланушысы есептік жазбаларының тізімінде көрсетіледі.

Kaspersky Security Center-ді бұлттық сегментте орналастырған кезде, IAM пайдаланушы есептік жазбасын пайдаланып жатқаныңызды көрсетіп, Kaspersky Security Center-ге қатынас кілтінің идентификаторы мен құпия қатынас кілтін беруіңіз қажет болады.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Amazon EC2 даналарына бағдарламаларды орнату үшін IAM рөлін құру

Kaspersky Security Center көмегімен EC2 даналарында қорғанысты орналастырмай тұрып, AWS басқару консолінде даналарға қолданбаларды орнату үшін қажетті құқықтары бар IAM рөлін жасаңыз. Кеңейтілген ақпарат IAM рөлдерін сипаттайтын AWS анықтамасы бөлімдерінде келтірілген.

IAM рөлі, оны Kaspersky Security Center көмегімен қауіпсіздік бағдарламаларын орнатуды жоспарлап отырған барлық EC2 даналарына тағайындау үшін қажет. Егер сіз данаға қажетті құқықтары бар IAM рөлін тағайындамасаңыз, бағдарламаларды осы даналарға AWS API құралдарымен орнату қатемен аяқталады.

AWS басқару консолімен жұмыс істеу үшін, сізге AWS есептік жазбасының пайдаланушы аты мен құпиясөзі керек.

Даналарға бағдарламаларды орнату мақсатымен IAM рөлін құру үшін:

1. AWS басқару консолі тармағын ашып, өзіңіздің AWS есептік жазбаңызбен кіріңіз.
2. Сол жақ мәзірден **Roles** тармағын таңдаңыз.

3. **Create Role** түймесін басыңыз.
4. Пайда болған сервистер тізімінен **EC2** тармағын таңдап, **Select Your Use case** тізімінен тағы да **EC2** тармағын таңдаңыз.
5. **Келесі: Құқықтар** түймесін басыңыз.
6. Пайда болған тізімде **AmazonEC2RoleforSSM** тармағына қарама-қарсы жалауша қойыңыз.
7. **Келесі: Қарау** түймесін басыңыз.
8. IAM рөлі атауы мен сипаттамасын енгізіп, **Create role** түймесін басыңыз.

   Жасалған рөл, сіз енгізген аты мен сипаттамасы бар рөлдер тізімінде көрсетіледі.

Алдағыда сіз Kaspersky Security Center көмегімен қорғайтын жаңа EC2 даналарын жасау кезінде құрылған IAM рөлін пайдалана аласыз, сондай-ақ оны бұрыннан бар даналармен байланыстыра аласыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Amazon RDS-пен жұмыс істеу

Бұл бөлімде Kaspersky Security Center үшін Amazon Relational Database Service (RDS) дерекқорын дайындау, оны параметрлер тобына орналастыру, RDS дерекқорымен жұмыс істеуге арналған IAM рөлін жасау, деректерді сақтауға арналған S3 орнын дайындау және дерекқорды қолданыстағы RDS дерекқорына тасымалдау үшін қандай қадамдар жасау керектігі сипатталған.

Amazon Relational Database Service (Amazon RDS) – бұл AWS пайдаланушыларына AWS бұлтты ортасында дерекқорды конфигурациялауға, басқаруға және масштабтауға мүмкіндік беретін веб-сервис. Сіз Amazon RDS дерекқорын Kaspersky Security Center бағдарламасымен жұмыс істеу үшін қолдана аласыз.

Сіз келесі дерекқорлармен жұмыс істей аласыз:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Amazon RDS данасын жасау

Amazon RDS данасын ДҚБЖ ретінде қолданғыңыз келсе, Amazon RDS дерекқор данасы жасай аласыз. Бұл бөлімде SQL Express Edition қалай таңдау керектігі сипатталған; егер сіз Aurora MySQL немесе Standard MySQL (5.7, 8.0 нұсқалары) қолданғыңыз келсе, сол өзектердің бірін таңдауыңыз қажет.

Amazon RDS дерекқор данасын жасау үшін:

1. AWS басқару консолін https://console.aws.amazon.com ашып, өзіңіздің есептік жазбаңызбен кіріңіз.
2. AWS интерфейсін пайдаланып, келесі параметрлермен дерекқор жасаңыз:
   - Өзек: Microsoft SQL Server, SQL Express Edition.
   - Дерекқорлар өзегінің нұсқасы: SQL Server 2014 12.00.5546.0v1.
   - Дерекқор үлгісі класы: db.t2.medium.
   - Сақтау орнының түрі: General purpose.
   - Сақтау орнының өлшемі: ең кемі 50 ГБ.
   - Қауіпсіздік тобы: Kaspersky Security Center Басқару сервері орнатылған EC2 данасы кіретін дәл сол топ.

   RDS данасы үшін идентификатор, пайдаланушы аты және құпиясөз жасаңыз.

   Сіз барлық әдепкі бойынша параметрлердің мәндерін қалдыра аласыз. Немесе Amazon RDS данасын конфигурациялағыңыз келсе, әдепкі бойынша параметр мәндерін өзгертіңіз. Толық ақпаратты AWS анықтама беттерінен қараңыз.
3. Соңғы қадамда, AWS процестің нәтижесін көрсетеді. Amazon RDS данасының толық ақпаратын көргіңіз келсе, **View DB instance details** түймесін басыңыз. Келесі әрекетке өткіңіз келсе, Amazon RDS данасы үшін параметрлер тобын жасаңыз.

Amazon RDS данасын жасауға бірнеше минут кетеді. Дана жасалғаннан кейін, сіз оны Kaspersky Security Center деректерімен жұмыс істеу үшін қолдана аласыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

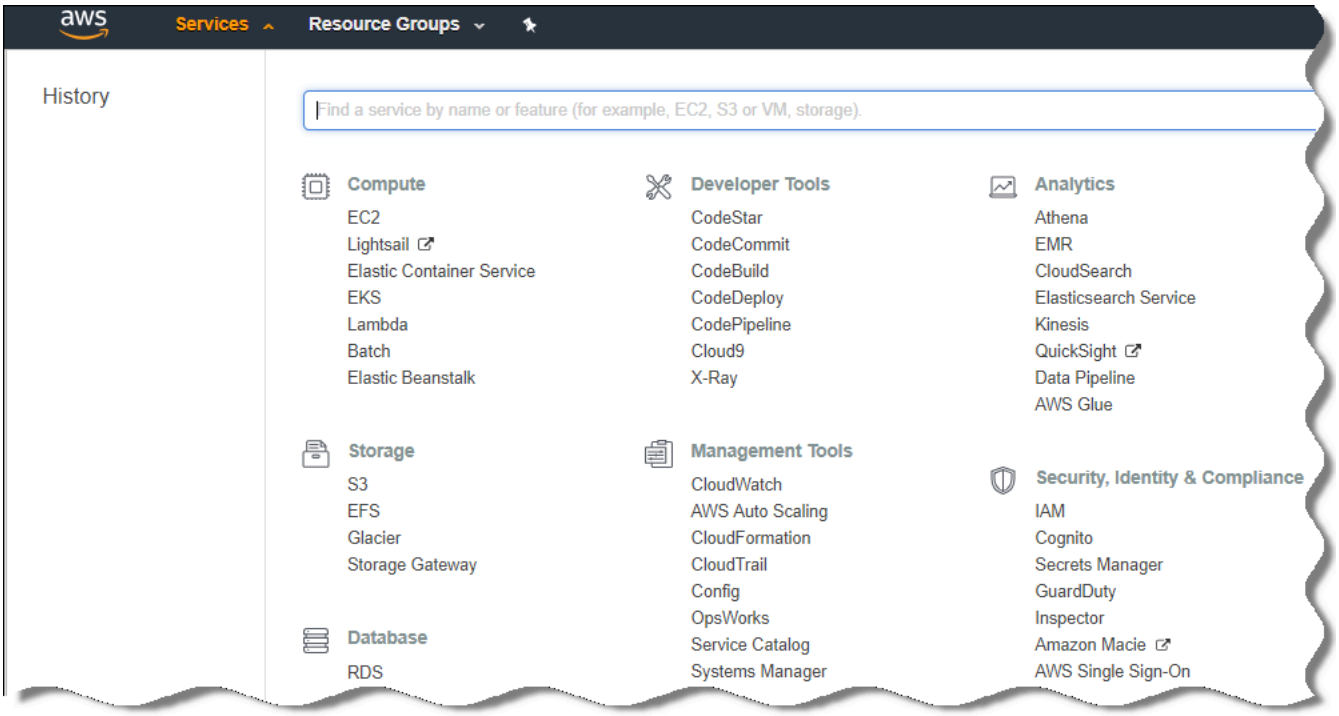
Amazon RDS данасы үшін параметрлер тобын құру

Amazon RDS данасын параметрлер тобына орналастыруыңыз керек.

Amazon RDS данасы үшін параметрлер тобын құру үшін:

1. AWS басқару консолі (https://console.aws.amazon.com) ашық екеніне және сіз есептік жазбаңызбен кіргеніңізге көз жеткізіңіз.
2. Мәзірден **Қызметтер** тармағын таңдаңыз.

   Қолжетімді қызметтер тізімі көрсетіледі (төмендегі суретті қараңыз).



AWS басқару консоліндегі қызметтер тізімі

3. Тізімнен **RDS** тармағын таңдаңыз.
4. Сол жақ тақтада **Option groups** түймесін басыңыз.
5. **Create group** түймесін басыңыз.
6. Келесі параметрлері бар параметрлер тобын жасаңыз (егер сіз Amazon RDS данасын жасау қадамында SQL Server серверін таңдасаңыз):
   - Өзек: SQLserver-ex.
   - Өзектің негізгі нұсқасы: 12.00.

   Amazon RDS данасын құру кезеңінде SQL емес дерекқорды таңдасаңыз, тиісті өзекті таңдаңыз.

Топ құрылды және топтар тізімінде көрсетіледі.

Параметрлер тобын жасағаннан кейін Amazon RDS данасын осы параметрлер тобына қойыңыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Параметрлер тобын өзгерту

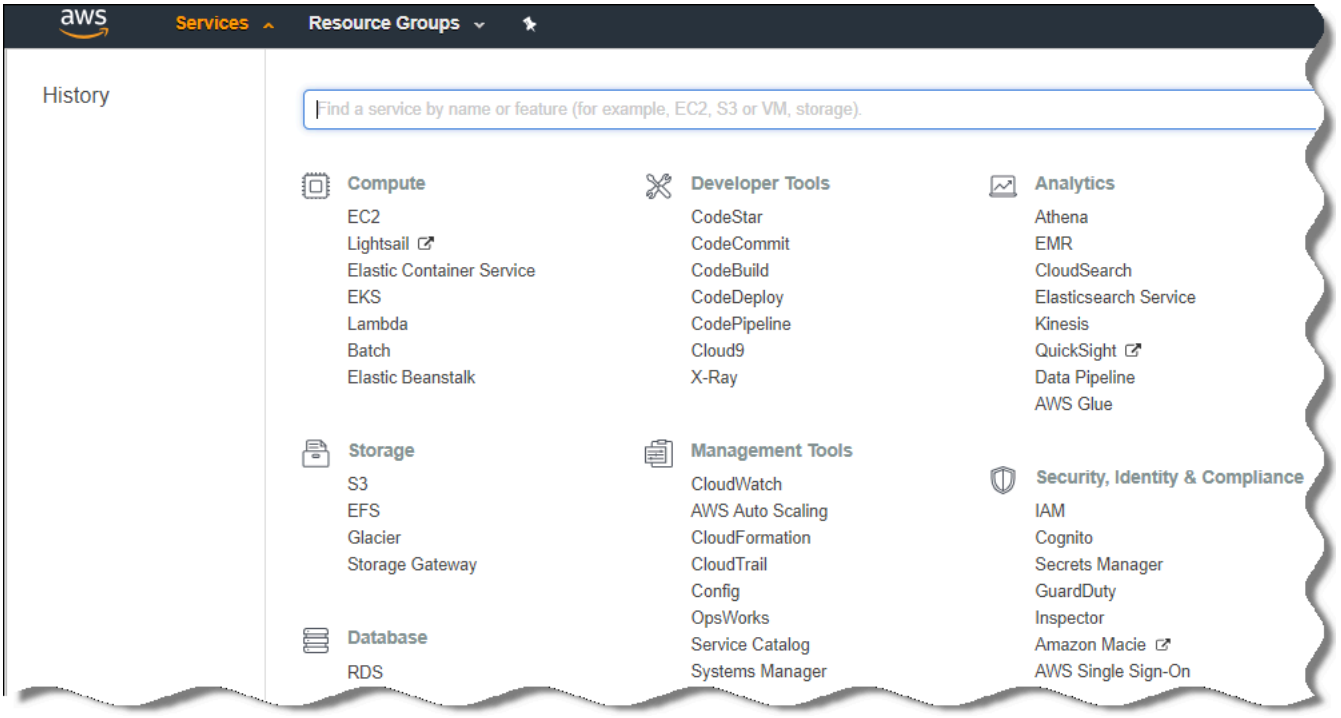
Amazon RDS данасын орналастырған параметрлер тобының әдепкі бойынша белгіленген конфигурациясы Kaspersky Security Center дерекқорымен жұмыс істеу үшін жеткіліксіз. Параметрлер тобына параметрлерді қосу және дерекқормен жұмыс істеу үшін IAM рөлін құру қажет.

Параметрлер тобын өзгерту және IAM рөлін құру:

1. AWS басқару консолі (https://console.aws.amazon.com) ашық екеніне және сіз есептік жазбаңызбен кіргеніңізге көз жеткізіңіз.

2. Мәзірден **Қызметтер** тармағын таңдаңыз.

   Қолжетімді қызметтер тізімі көрсетіледі (төмендегі суретті қараңыз).



AWS басқару консолиндегі қызметтер тізімі

3. Тізімнен RDS тармағын таңдаңыз.

4. Сол жақ тақтада **Option groups** түймесін басыңыз.

   Параметр топтарының тізімі көрсетіледі.

5. Amazon RDS данасы орналастырылған параметрлер тобын таңдап, **Параметрді қосу** түймесін басыңыз.

   Параметрді қосу терезесі ашылады.

6. IAM рөлі бөлімінде **Create a new role** / **Yes** параметрін таңдап, жаңа IAM рөлінің атауын енгізіңіз.

   Рөл әдепкі бойынша құқықтар жиынтығымен бірге жасалған. Кейінірек, осы құқықтарды өзгерте аласыз.

7. S3 орны бөлімінде келесі әрекеттердің бірін орындаңыз:

   - Сақтық көшірме үшін Amazon S3 орнының данасы жасалмаса, **S3 орнын жасау** сілтемесінен өтіп, AWS интерфейсі арқылы S3 орнын жасаңыз.
   - Басқару сервері деректерінің сақтық көшірмесін жасау үшін Amazon S3 орнының данасын жасап қойған болсаңыз, ашылмалы мәзірден қажетті S3 орнын таңдаңыз.

8. Параметрлерді қосуды аяқтау үшін беттің төменгі жағындағы **Параметрді қосу** түймесін басыңыз.

Сіз параметрлер тобын өзгерттіңіз және RDS дерекқорымен жұмыс істеу үшін IAM рөлін жасадыңыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Amazon RDS дерекқор данасы үшін IAM рөлі құқықтарын өзгерту

Параметрлерді параметрлер тобына қосқаннан кейін, сізге Amazon RDS дерекқор данасымен жұмыс істеу үшін жасалған IAM рөлінің қажетті құқықтарын тағайындау керек.

Amazon RDS дерекқор данасымен жұмыс істеу үшін жасаған қажетті IAM рөлдерін тағайындау үшін:

1. AWS басқару консолі (https://console.aws.amazon.com) ашық екеніне және сіз есептік жазбаңызбен кіргеніңізге көз жеткізіңіз.
2. Қызметтер тізімінен **IAM** таңдаңыз.

   Пайдаланушы аттары тізімі мен құралмен жұмыс істеуге болатын мәзірі бар терезе ашылады.
3. Мәзірден **Рөлдер** тармағын таңдаңыз.
4. IAM рөлдері тізімінен параметрлерді параметрлер тобына қосу уақытында жасалған рөлді таңдаңыз.
5. AWS интерфейсін қолдана отырып, **sqlNativeBackup-<date>** саясатын жойыңыз.
6. AWS интерфейсін қолдана отырып, рөлдің **AmazonS3FullAccess** саясатын тағайындаңыз.

IAM рөлі Amazon RDS-пен жұмыс істеу үшін қажетті құқықтарды алады.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Дерекқор үшін Amazon S3 себетін дайындау

Егер сіз Amazon Relational Database System (Amazon RDS) дерекқорын пайдалануды жоспарласаңыз, сізге әдеттегі деректердің сақтық көшірмесін сақтайтын Buzz Amazon Simple Storage Service (Amazon S3) себетінің данасын жасау қажет болады. Amazon S3 туралы және S3 себеттері туралы толық ақпаратты Amazon анықтамасынан ала аласыз. Amazon S3 данасын жасау туралы толық ақпаратты Amazon S3 анықтамасынан ала аласыз.

Amazon S3 себетін жасау үшін:

1. AWS басқару консолі ашық екеніне және сіз есептік жазбаңызбен кіргеніңізге көз жеткізіңіз.
2. AWS қызметтері тізімінен S3 таңдаңыз.
3. Себетті жасау үшін консольге өтіп, шебердің нұсқауларын орындаңыз.
4. Басқару сервері орналасқан (немесе орналасатын) аймақты таңдаңыз.
5. Соңғы қадамда себеттер тізімінде жаңа себеттің пайда болғанына көз жеткізіңіз.

S3 себеті жасалды және себеттер тізімінде көрсетіледі. Параметрді параметрлер тобына қосу кезінде себетті көрсете аласыз. Сондай-ақ, Kaspersky Security Center-де *Басқару сервері деректерінің резервтік қоймасы* тапсырмасын жасау кезінде Kaspersky Security Center-де S3 себетіңіздің мекенжайын да көрсете аласыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Дерекқорды Amazon RDS-ке тасымалдау

Сіз Kaspersky Security Center дерекқорыңызды жергілікті құрылғыдан Amazon RDS қолдайтын Amazon S3 данасына тасымалдай аласыз. Бұл мақсатта, RDS дерекқоры үшін S3 себеті және осы S3 себеті үшін AmazonS3FullAccess құқықтары бар IAM пайдаланушысының есептік жазбасы керек.

Дерекқорды тасымалдау үшін:

1. RDS данасын жасағаныңызға көз жеткізіңіз (толық ақпаратты Amazon RDS анықтамалық беттерінен ала аласыз).
2. Физикалық Басқару серверіңізде (жергілікті), Басқару сервері деректері үшін Kaspersky сақтық көшірмелеу утилитасын іске қосыңыз.

   Файлдың атауы backup.zip екеніне көз жеткізіңіз.
3. backup.zip сақтық көшірме файлын Басқару сервері орнатылған EC2 данасына көшіріп алыңыз.

   Басқару сервері орнатылған EC2 данасында бос диск кеңістігінің жеткілікті екеніне көз жеткізіңіз. AWS айналасында дерекқорды тасымалдау процесін орындау үшін данаңызға диск кеңістігін қосуға болады.
4. AWS-тағы Басқару серверінде Kaspersky сақтық көшірмелеу утилитасын интерактивті емес режимде қайтадан іске қосыңыз.

   Нәтижесінде, деректерді сақтық көшірмелеу және қалпына келтіру шебері іске қосылады.
5. **Әрекетті таңдау** қадамында **Басқару серверінің деректерін қалпына келтіру** тармағын таңдап, **Келесі** түймесін басыңыз.
6. **Қалпына келтіру параметрлері** қадамында **Сақтық көшірмелерді сақтауға арналған қалта** өрісінің жанындағы **Шолу** түймесін басыңыз.

7. Ашылған **Онлайн сақтау орнына кіру** терезесінде келесі өрістерді толтырып, **OK** түймесін басыңыз:

   - **S3 орнының атауы**

     S3 орнының атауы.

   - **Резервтік қойма қалтасы**

     Сақтық көшірмелерді сақтауға арналған қалтаның орналасуын көрсетіңіз.

   - **Қатынас кілтінің идентификаторы**

     Amazon S3 орнын пайдалану құқығы (AmazonS3FullAccess құқықтары) бар IAM пайдаланушысына тиесілі AWS IAM қатынас кілті.

   - **Құпия кілт**

     Amazon S3 орнын пайдалану құқығы (AmazonS3FullAccess құқықтары) бар IAM пайдаланушысына тиесілі AWS IAM құпия кілті.

8. **Жергілікті сақтық көшірмеден тасымалдау** параметрін таңдаңыз. **Шолу** түймесін қолжетімді болады.

9. **Шолу** түймесін басып, AWS Басқару серверінде backup.zip файлы орналастырылған қалтаны таңдаңыз.

10. **Келесі** түймесін басып, процедураны аяқтаңыз.

Деректер S3 орнын пайдалану арқылы RDS дерекқорында сақталады. Сіз бұл дерекқорды AWS айналасында Kaspersky Security Center бағдарламасымен одан әрі жұмыс істеу үшін пайдалана аласыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Microsoft Azure бұлтты ортасында жұмыс істеу

Бұл бөлімде Kaspersky Security Center бағдарламасын Microsoft Azure платформасы ұсынған бұлтты ортада қалай орналастыруға және қолдауға болатындығы, сондай-ақ виртуалды машиналарда қорғанысты бұлтты ортада қалай орналастыруға болатындығы туралы ақпарат берілген.

Қызмет көлеміне байланысты ай сайынғы тарифтік жазылымды қолдана отырып орналастырылған Kaspersky Security Center бағдарламасында Осалдықтар мен патчтарды басқару мүмкіндіктері автоматты түрде белсендіріледі, бірақ Ұялы құрылғыларды басқаруды белсендіру мүмкін емес.

Microsoft Azure жүйесінде жұмыс істеу туралы

Microsoft Azure платформасымен жұмыс істеу үшін, атап айтқанда Azure Marketplace дүкенінен бағдарламалар сатып алу және виртуалды машиналар жасау үшін сізге Azure жазылымы қажет. Басқару серверін орналастырмас бұрын, виртуалды машиналарға бағдарламаларды орнату үшін қажетті құқықтары бар Azure бағдарламаның идентификаторын жасаңыз.

Azure Marketplace дүкенінен Kaspersky Security Center кескінін сатып алсаңыз, Kaspersky Security Center Басқару серверінің AMI дайын кескіні бар виртуалды машинаны орналастыра аласыз. Виртуалды машинаның параметрлерін таңдау керек, бірақ бағдарламаларды өз бетінше орнатудың керегі жоқ. Орнатқаннан кейін, сіз Басқару консолін іске қосып, Kaspersky Security Center бағдарламасымен жұмысты бастау үшін Басқару серверіне қосыла аласыз.

Сондай-ақ, физикалық құрылғыларды қорғау үшін Kaspersky Security Center Басқару сервері бар Azure виртуалды машинасын пайдалануға болады (мысалы, мұндай бұлтты сервер физикалық серверге қарағанда техникалық қызмет көрсету мен күтіп ұстауда тиімдірек болса). Бұл жағдайда, Басқару серверімен атқарылатын жұмыс, физикалық құрылғыға орнатылған Басқару серверіндей жүзеге асырылатын болады. Azure API құралдарын пайдалануды жоспарламасаңыз, Azure бағдарламаның идентификаторы қажет емес. Бұл жағдайда, Azure жазылымы жеткілікті.

Жазылымды, бағдарлама идентификаторын және құпиясөзді жасау

Microsoft Azure ортасында Kaspersky Security Center бағдарламасымен жұмыс істеу үшін, сізге Azure жазылымы, Azure бағдарламаның идентификаторы және Azure бағдарлама құпиясөзі керек. Егер сізде жазылым бар болса, оны пайдалана аласыз.

Azure жазылымы өзінің иесіне Microsoft Azure Platform Management Portal порталына және Microsoft Azure сервистеріне қол жеткізуге мүмкіндік береді. Иесі Azure SQL және Azure Storage сияқты қызметтерді басқару үшін Microsoft Azure Platform қолдана алады.

Microsoft Azure жазылымын жасау үшін,

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription сайтына өтіңіз және нұсқауларды орындаңыз.

Жазылым жасау туралы толық ақпарат Microsoft сайтында қолжетімді. Сіз жазылым идентификаторын алып, Kaspersky Security Center бағдарламасына қолданба идентификаторымен және құпиясөзбен бірге бересіз.

Қолданба идентификаторы мен Azure бағдарлама құпиясөзін жасау және сақтау үшін:

1. https://portal.azure.com сілтемесінен өтіп, кіруді орындағаныңызға көз жеткізіңіз.
2. Анықтама бетіндегі нұсқауларды орындай отырып, қолданба идентификаторын жасаңыз.
3. Бағдарлама сипаттарында **Keys** бөліміне өтіңіз.
4. **Keys** бөлімінде **Description** және **Expires** өрістерін толтырып, **Value** өрісін бос қалдырыңыз.
5. **Сақтау** түймесін басыңыз.

   Save түймесін басқаннан кейін, жүйе **Value** өрісін таңбалардың ұзын тізбегімен автоматты түрде толтырады. Бұл таңбалар тізбегі Azure қолданбасының құпиясөзі болып табылады (мысалы, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). Сипаттама сіз көрсеткендей көрсетіледі.

6. Құпиясөзді көшіріп, кейінірек Kaspersky Security Center бағдарламасына қолданба идентификаторы мен құпиясөзді бере алатындай етіп сақтап қойыңыз.

   Құпиясөзді жасаған кезде ғана көшіруге болады. Кейінірек, құпиясөз бұдан былай көрсетілмейді және сіз оны қалпына келтіре алмайсыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Azure бағдарламаның идентификаторы үшін рөлді тағайындау

Егер құрылғыны табу процесі арқылы виртуалды машиналарды табу қажет болса, Azure бағдарламаның идентификаторына Оқырман (Reader) рөлі тағайындалуы керек. Егер виртуалды машиналарды тауып қана қоймай, виртуалды машиналарда қорғауды жою қажет болса, Azure бағдарламаның идентификаторына Виртуалды машина қатысушысы (Virtual Machine Contributor) рөлі тағайындалуы керек.

Azure бағдарламаның идентификаторына рөлді тағайындау үшін Microsoft веб-сайтында келтірілген нұсқауларды орындаңыз.

Microsoft Azure жүйесінде Басқару серверін орналастыру және дерекқорды таңдау

Microsoft Azure ортасында Басқару серверін орналастыру үшін:

1. Есептік жазбаңызды пайдаланып, Microsoft Azure жүйесіне кіріңіз.
2. Azure порталына өтіңіз.
3. Тақтаның сол жағында плюс жасыл белгішесін басыңыз.
4. Мәзірдің іздеу өрісінде "Kaspersky Hybrid Cloud Security" деп жазыңыз.

   Kaspersky Hybrid Cloud Security – бұл Kaspersky Security Center және даналарды қорғауға арналған екі қауіпсіздік бағдарламасының тіркесімі: Kaspersky Endpoint Security for Linux және Kaspersky Security for Windows Server.
5. Нәтижелер тізімінен Kaspersky Hybrid Cloud Security немесе Kaspersky Hybrid Cloud Security (BYOL) таңдаңыз.

   Экранның оң жағында ақпараттық терезе көрсетіледі.
6. Ақпаратты оқып, ақпараттық терезеде Жасау түймесін басыңыз.
7. Қажетті өрістерді толтырыңыз. Ақпарат пен көмек алу үшін кеңестер мен анықтаманы пайдаланыңыз.
8. Өлшемді таңдағанда үш параметрдің бірін таңдаңыз.

   Көп жағдайда 8 ГБ жедел жады жеткілікті. Azure порталында сіз кез келген уақытта виртуалды машинада жедел жад пен басқа ресурстардың көлемін ұлғайта аласыз.

9. Дерекқорды таңдағанда, жоспарыңызға сәйкес келесі нұсқалардың бірін таңдаңыз:

   - Жергілікті — дерекқордың басқару сервері орналастырылатын виртуалды машинада болғанын қаласаңыз. Kaspersky Security Center бағдарламасы SQL Server Express дерекқорымен бірге жеткізіледі. Егер SQL Server Express дерекқоры сіздің қажеттіліктеріңізге жеткілікті болса, осы параметрді таңдаңыз.

   - Жаңа — жаңа RDS дерекқорының Azure ортасында болғанын қаласаңыз. SQL Server Express-тен басқа ДҚБЖ қолданғыңыз келсе, осы опцияны таңдаңыз. Сіздің деректеріңіз бұлтты ортаға көшіріліп, сонда қалады және сізде қосымша шығындар болмайды.

   - Бұрыннан бар — бұрыннан бар дерекқор серверін пайдаланғыңыз келсе. Бұл жағдайда оның орналасқан жерін көрсетуіңіз керек. Егер сервер Azure ортасынан тыс болса, сіздің деректеріңіз интернет арқылы көшіріліп, бұл қосымша шығындарға әкелуі мүмкін.

10. Жазылым идентификаторын енгізген кезде бұрын жасалған жазылымды пайдаланыңыз.

Орналастырылғаннан кейін, сіз RDP көмегімен Басқару серверіне қосыла аласыз. Басқару серверімен жұмыс істеу үшін Басқару консолін пайдалануға болады.

Azure SQL-мен жұмыс істеу

Бұл бөлімде Microsoft Azure дерекқорын Kaspersky Security Center бағдарламасын пайдалануға дайындауға, сондай-ақ Azure сақтау тіркелгісін дайындауға және қолданыстағы дерекқорды Azure SQL-ге тасымалдауға қажетті әрекеттер сипатталған.

SQL дерекқоры – бұл Microsoft Azure-дағы реляциялық дерекқорларды басқарудың әмбебап қызметі.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Azure сақтау тіркелгісін жасау

Microsoft Azure жүйесінде Azure SQL дерекқорымен жұмыс істеу үшін және орналастыру скрипттері үшін сақтау тіркелгісін жасау қажет.

Сақтау тіркелгісін жасау үшін:

1. Azure порталына кіріңіз.

2. Сол жақ тақтадан **Сақтау тіркелгілері** тармағын таңдап, **Сақтау тіркелгілері** терезесіне өтіңіз.

3. **Сақтау тіркелгісін жасау** терезесіне өту үшін **Сақтау тіркелгілері** терезесінде **Қосу** түймесін басыңыз.

4. Сақтау тіркелгісін жасау үшін барлық қажетті өрістерді толтырыңыз:

   - Орналасқан жері: Басқару серверінің орналасқан жеріне (географиялық аймаққа) сәйкес келуі керек.

   - Басқа өрістер: әдепкі бойынша көрсетілген мәндерді қалдыруға болады.

Әрбір өріс туралы ақпарат алу үшін кеңестерді пайдаланыңыз.

Сақтау тіркелгісін жасағаннан кейін, сақтау тіркелгілері тізімі көрсетіледі.

5. Сақтау тіркелгілері тізімінде, ол туралы ақпаратты көру үшін, жасалған тіркелгіні бөлектеңіз.

6. Тіркелгінің атауын, ресурстар тобын және сол сақтау тіркелгісінің қатынас кілттерін білетіндігіңізге көз жеткізіңіз. Бұл деректер сізге Kaspersky Security Center-мен жұмыс істеу кезінде қажет болады.

Анықтаманы Azure веб-сайтында қарауға болады.

Егер сізде сақтау тіркелгісі болса, оны Kaspersky Security Center-мен жұмыс істеу үшін пайдалануға болады.

Azure SQL дерекқоры мен SQL серверін құру

Azure айналасында сізге SQL дерекқоры мен SQL сервері қажет.

Azure SQL дерекқоры мен SQL серверін құру үшін:

1. Azure веб-сайтында келтірілген нұсқауларды орындаңыз.

   Microsoft Azure сұраған кезде, жаңа сервер жасауға болады; Azure SQL сервері бар болса, оны жаңасын жасаудың орнына Kaspersky Security Center үшін пайдалануға болады.

2. SQL дерекқоры мен SQL серверін жасағаннан кейін, ресурс атауы мен ресурстар тобын білетініңізге көз жеткізіңіз.

   a. https://portal.azure.com сілтемесінен өтіп, кіруді орындағаныңызға көз жеткізіңіз.

   b. Сол жақ тақтадан **SQL дерекқоры** тармағын таңдаңыз.

   c. Дерекқорлар тізімінен дерекқор атауын таңдаңыз.

      Сипаттар терезесі ашылады.

   d. Дерекқордың атауы ресурстың атауы болып саналады. Ресурстар тобының атауы **Шолу** бөліміндегі сипаттар терезесінде көрсетіледі.

Дерекқорды Azure SQL-ге тасымалдау кезінде сізге ресурс атауы және дерекқор ресурстарының тобы қажет болады.

Дерекқорды Azure SQL-ге тасымалдау

Microsoft Azure айналасында Басқару серверін орналастырғаннан кейін, Kaspersky Security Center дерекқорын физикалық құрылғыдан Azure SQL-ге тасымалдауға болады. Azure SQL дерекқорын пайдалану үшін Azure сақтау тіркелгісі қажет. Сондай-ақ, сізде Microsoft SQL Server және Басқару серверіңізде SQLSysCLRTypes және деректер деңгейі (Dacfx) қолданбасы платформасы болуы керек.

Дерекқорды тасымалдау үшін:

1. Azure сақтау тіркелгісін жасағаныңызға көз жеткізіңіз.

2. Басқару серверінде SQLSysCLRTypes және DacFx бар екеніне көз жеткізіңіз.

   Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) және SQLSysCLRTypes (SQL Server серверіңіздің нұсқасына сәйкес нұсқаны таңдаңыз) қолданбаларын Microsoft ресми сайтынан жүктей аласыз.

3. Физикалық Басқару серверіңізде, **Azure пішіміне ауысу** параметрі қосулы Басқару сервері деректері үшін Kaspersky сақтық көшірмелеу утилитасын іске қосыңыз.

4. Деректердің сақтық көшірме файлын Azure ішіндегі Басқару серверіне салыңыз.

   Басқару сервері орнатылған Azure виртуалды машинасында бос диск кеңістігінің жеткілікті екеніне көз жеткізіңіз. Azure айналасында дерекқорды тасымалдау процесін қамтамасыз ету үшін виртуалды машинаға арналған диск кеңістігін қосуға болады.

5. Microsoft Azure бұлтты ортасында орналасқан Басқару серверінде Kaspersky сақтық көшірмелеу утилитасын интерактивті режимде тағы бір рет іске қосыңыз.

   Нәтижесінде, деректерді сақтық көшірмелеу және қалпына келтіру шебері іске қосылады.

6. **Әрекетті таңдау** қадамында **Басқару серверінің деректерін қалпына келтіру** тармағын таңдап, **Келесі** түймесін басыңыз.

7. **Қалпына келтіру параметрлері** қадамында **Сақтық көшірмелерді сақтауға арналған қалта** өрісінің жанындағы **Шолу** түймесін басыңыз.

8. Ашылған **Онлайн сақтау орнына кіру** терезесінде келесі өрістерді толтырып, **OK** түймесін басыңыз:

   - **Azure сақтау орнының есептік жазба атауы**

     Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

   - **Резервтік қойма қалтасы**

     Сақтық көшірмелерді сақтауға арналған қалтаның орналасуын көрсетіңіз.

   - **Azure жазылым идентификаторы**

     Azure порталында жазылым жасадыңыз.

   - **Azure бағдарлама құпиясөзі.**

     Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

     Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

   - **Azure сақтау орнының қатынас кілті**

     "Access Keys" бөлімінде сақтаудың есептік жазбасы сипаттарында қолжетімді. Кез келген кілтті қолдана аласыз (key1 немесе key2).

   - **Azure SQL сервері атауы**

     Azure SQL серверінің сипаттарында қолжетімді.

   - **Azure SQL серверінің ресурстық тобы**

     Azure SQL серверінің сипаттарында қолжетімді.

   - **Azure бағдарламасының идентификаторы.**

     Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

9. **Жергілікті сақтық көшірмеден тасымалдау** параметрін таңдаңыз.

   Шолу түймесін қолжетімді болады.

10. **Шолу** түймесін басып, Azure-дағы Басқару серверінен деректердің сақтық көшірме файлы орналастырылған қалтаны таңдаңыз.

11. **Келесі** түймесін басып, процедураны аяқтаңыз.

Деректер Azure қоймасын пайдаланып, Azure SQL дерекқорына қалпына келтіріледі. Сіз бұл дерекқорды Azure айналасында Kaspersky Security Center-пен одан әрі жұмыс істеу үшін пайдалана аласыз.

Осы құжатта көрсетілген веб-беттердің мекенжайлары Kaspersky Security Center шыққан күні дұрыс болып саналады.

Google Cloud бұлтты ортасында жұмыс істеу

Бұл бөлімде Google ұсынатын бұлтты ортада Kaspersky Security Center бағдарламасымен жұмыс істеу туралы ақпарат бар.

Клиенттің электрондық поштасын, жоба идентификаторын және жеке кілтті жасау

Google API интерфейсін Google Cloud платформасында Kaspersky Security Center бағдарламасымен жұмыс істеу үшін пайдалануға болады. Google есептік жазбасы қажет. Кеңейтілген ақпаратты https://cloud.google.com бетіндегі Google құжаттамасынан таба аласыз.

Сізге Kaspersky Security Center бағдарламасына келесі есептік деректерін жасау және ұсыну қажет:

- **Клиенттің электрондық поштасы**

  Клиенттің электрондық поштасы – бұл сіздің жобаңызды Google Cloud-қа тіркеу үшін пайдаланған электрондық пошта мекенжайы.

- **Жоба идентификаторы**

  Жоба идентификаторы – бұл Google Cloud жобасын тіркеу кезінде алынған идентификатор.

- **Жеке кілт**

  Жеке кілт – бұл жобаны Google Cloud-қа тіркеу кезінде жеке кілт ретінде алынған таңбалар бірізділігі. Қателерді болдырмау үшін осы бірізділікті көшіруге және қоюға болады.

MySQL үшін Google Cloud SQL данасымен жұмыс істеу

Сіз Google Cloud бұлтты ортасында дерекқор құра аласыз және осы дерекқорды Kaspersky Security Center үшін пайдалана аласыз.

Kaspersky Security Center бағдарламасы MySQL 5.7 және 5.6 нұсқаларымен жұмыс істейді. MySQL басқа нұсқалары сыналған жоқ.

MySQL дерекқорын құру және конфигурациялау үшін:

Браузерде https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen бетін ашып, нұсқауларды орындаңыз.

MySQL дерекқорын конфигурациялаған кезде келесі жалаушаларды қолданыңыз:

- **sort_buffer_size** 10000000;
- **join_buffer_size** 20000000;
- **innodb_lock_wait_timeout** 300;
- **max_allowed_packet** 32000000;
- **innodb_thread_concurrency** 20;
- **max_connections** 151;
- **tmp_table_size** 67108864;
- **max_heap_table_size** 67108864;
- **lower_case_table_names** 1.

Kaspersky Security Center-мен жұмыс істеу үшін бұлтты ортада клиент құрылғыларын дайындау

Сіз Kaspersky Басқару серверін, Желілік агентін және қауіпсіздік бағдарламаларын орнатуды жоспарлап отырған құрылғылар келесі шарттарға сәйкес келуі керек:

- Қауіпсіздік топтарының конфигурациялары Басқару серверіндегі келесі порттарды қолжетімді етеді (орналастыру үшін ең аз қажет порттар жиынтығы):
  - 8060 HTTP – Басқару серверінен Желілік агенттің орнату пакеттері мен қауіпсіздік бағдарламаларының қорғалатын даналарына беру үшін;
  - 8061 HTTP – Басқару серверінен Желілік агенттің орнату пакеттері мен қауіпсіздік бағдарламаларының қорғалатын даналарына беру үшін;

- 13000 TCP – қорғалған даналардан және қосалқы Басқару серверлерінен SSL көмегімен негізгі Басқару серверіне беру үшін;
- 13000 UDP – даналарды өшіру туралы ақпаратты Басқару серверіне беру үшін;
- 14000 TCP – қорғалған даналардан және қосалқы Басқару серверлерінен SSL-сіз негізгі Басқару серверіне беру үшін;
- 13291 – Басқару консолін Басқару серверіне қосу үшін;
- 40080 – орналастыру скрипттері жұмыс істеуі үшін.

Қауіпсіздік топтарын AWS басқару консолінде немесе Azure порталында конфигурациялауға болады. Kaspersky Security Center бағдарламасын әдепкі емес конфигурацияда пайдаланғыңыз келсе, Білім қорын қараңыз. Әдепкі конфигурациялардан басқа конфигурациялардың мысалдары, Басқару сервері бар құрылғыға Басқару консолін орнатуды қамтымайды, бірақ жұмыс станцияңызға KSN прокси-серверін орнатуды немесе пайдалануды қамтиды.

- Клиент құрылғыларында 15000 UDP порты қолжетімді (Басқару сервермен байланысуға сұраулар қабылдау үшін).
- AWS бұлтты ортасында:
  - AWS API-ді қолдануды жоспарласаңыз, онда даналарда бағдарламалар орнатылатын IAM рөлі белгіленеді.
  - Әрбір Amazon EC2 данасында Systems Manager Agent (SSM агенті) орнатылған және іске қосылған.
  - SSM агенті Kaspersky Security Center-ге әрбір рет әкімшіден растауды сұрамай-ақ, бағдарламаларды құрылғылар мен құрылғылар топтарына автоматты түрде орнатуға мүмкіндік береді.
  - 2016 жылдың қараша айынан кейінгі AMI кескіндерінен орналастырылған Windows операциялық жүйесі басқаратын даналарда SSM агенті орнатылып, жұмыс істейді. Барлық басқа құрылғыларда SSM агентін өзіңіз орнатуыңыз керек. Windows және Linux операциялық жүйелері басқаратын құрылғыларға SSM агентін орнату туралы көбірек білу үшін AWS анықтама бетін қараңыз.
- Microsoft Azure бұлтты ортасында:
  - Әрбір Azure виртуалды машинасында Azure VM Agent орнатылған және іске қосылған.

    Әдепкі бойынша, виртуалды машина Azure VM Agent-пен бірге жасалады және оны қолмен орнатуға немесе қосуға тиіс емессіз. Windows құрылғыларында және Linux құрылғыларында Azure VM Agent туралы қосымша ақпарат алу үшін Microsoft анықтама беттерін қараңыз.
  - Сіздің Azure есептік жазбасының атауы келесі рөлдерге ие:
    - Оқырман (желіде сауалнама өткізу кезінде виртуалды машиналарды анықтайды).
    - Виртуалды машинаның қатысушысы (виртуалды машиналарда қорғанысты қолданады).
    - SQL Server Contributor (Microsoft Azure бұлтты ортасында SQL дерекқорын пайдаланады).

    Осы операциялардың барлығын орындағыңыз келсе, барлық үш рөлді Azure бағдарламасының идентификаторына тағайындаңыз.

Бұлтты ортаны конфигурациялау үшін қажетті орнату пакеттерін жасау

Kaspersky Security Center бағдарламасындағы бұлтты ортаны конфигурациялау шебері келесі бағдарламалар үшін орнату пакеттері мен басқару плагиндері болса, қолжетімді болады:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  > Kaspersky Endpoint Security for Windows жүйесін бұлттық ортада орналастыру Kaspersky Endpoint Security 12.0 for Windows нұсқасы шыққаннан кейін қолжетімді болады.

- Kaspersky Security for Windows Server

Бұл орнату пакеттері сіз қорғағыңыз келетін даналарға және виртуалды машиналарға бағдарламаларды орнату үшін қажет. Бұл орнату пакеттері болмаса, оларды жасауыңыз керек. Әйтпесе, бұлтты ортаны конфигурациялау шебері іске қосылмайды.

Орнату пакеттерін жасау үшін:

1. Бағдарламалар мен плагиндердің соңғы нұсқаларын Kaspersky сайтынан жүктеп алыңыз:
   - Windows Server серверіне арналған Kaspersky Security бағдарламасына арналған орнатушы және басқару плагині.
   - Орнатушы, Kaspersky Security Center арқылы қашықтан орнатуға арналған файлдар және Kaspersky Endpoint Security for Linux басқару плагині.
2. Басқару сервері орнатылған данаға (немесе виртуалды машинаға) барлық файлдарды сақтаңыз.
3. Барлық пакеттерден файлдарды шығарып алыңыз.
4. Kaspersky Security Center іске қосыңыз.
5. Консоль ағашында **Кеңейтілген** → **Қашықтан орнату** → **Орнату пакеттері** бөліміне өтіп, **Орнату пакетін жасау** түймесін басыңыз.
6. **Kaspersky орнату пакетін жасау** тармағын таңдаңыз.
7. Пакеттің атауын және бағдарлама орнатушысының жолын көрсетіңіз: <folder>\<file name>.kud және **Келесі** түймесін басыңыз.
8. Лицензиялық келісімді оқып шығыңыз, оның шарттарын қабылдағаныңызды растайтын жалаушаны қойыңыз және **Келесі** түймесін басыңыз.

Орнату пакеті Басқару серверіне жүктелді және орнату пакеттерінің тізімінде қолжетімді.

Бұлтты ортаны конфигурациялау, орнату пакеттерін жасаған кезде және Басқару серверінде басқару плагиндерін орнатқан кезде қолжетімді болады.

Бұлтты ортаны конфигурациялау

Бұлтты ортаны конфигурациялау шеберін пайдаланып Kaspersky Security Center конфигурациялау үшін сізге мыналар қажет:

- Бұлтты орта үшін есептік деректерді көрсетіңіз:
  - Бұлттық сегментте сауалнама өткізу құқығы ұсынылған IAM рөлі немесе бұлттық сегментте сауалнама өткізу құқығы ұсынылған IAM пайдаланушысының есептік жазбасы (Amazon Web Services қызметімен жұмыс істеу үшін);
  - Azure бағдарламасының идентификаторы, құпиясөз және жазылым (Microsoft Azure-мен жұмыс істеу үшін);
  - Google клиентінің электрондық поштасы, жобаның идентификаторы және жабық кілт (Google Cloud-пен жұмыс істеу үшін).
- Орнату пакеттері:
  - Windows үшін Желілік агент
  - Linux үшін Желілік агент
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux веб-плагині
- Кемінде келесілердің бірі:
  - Kaspersky Endpoint Security for Windows орнату пакеті және веб-плагині (ұсынылады)
  - Kaspersky Security for Windows Server орнату пакеті және веб-плагині

Бұлтты ортада жұмыс істеу мүмкіндіктерін пайдаланғыңыз келмесе (мысалы, тек физикалық клиент құрылғыларының қауіпсіздігін басқарғыңыз келсе), бұлтты ортаны конфигурациялау шеберінен шығып, стандартты Басқару серверін жылдам іске қосу шеберін қолмен іске қоса аласыз.

Kaspersky Security Center бағдарламасын дайын AMI кескінінен орналастырып жатсаңыз, Басқару серверіне Басқару консолі арқылы алғаш қосылған кезде бұлтты ортаны конфигурациялау автоматты түрде басталады. Сондай-ақ, бұлтты ортаны конфигурациялау шеберін кез келген уақытта іске қоса аласыз.

Бұлтты ортаны конфигурациялау шеберін қолмен іске қосу үшін:

1. Консоль ағашынан **Басқару сервері** түйінін таңдаңыз.
2. Түйіннің мәнмәтіндік мәзірінде **Барлық тапсырмалар → Бұлт ортасын конфигурациялау** тармағын таңдаңыз.

Конфигурациялау уақыты шамамен 15 минут.

Бұлтты ортаны конфигурациялау шебері туралы

Бұлтты ортаны конфигурациялау шебері бұлтты ортадағы жұмыс ерекшеліктерін ескере отырып, Kaspersky Security Center-ді конфигурациялауға мүмкіндік береді.

Шебердің жұмысы нәтижесінде келесі нысандар жасалады:

- әдепкі конфигурациялары бар Желілік агент саясаты;
- Kaspersky Endpoint Security for Linux саясаты;
- Kaspersky Security for Windows Server саясаты;
- басқару тобы және даналарды осы басқару тобына автоматты түрде жылжыту ережесі;
- Басқару сервері деректерін сақтық көшірмелеу тапсырмасы;
- Linux және Windows басқаратын құрылғыларға қорғанысты орнату тапсырмалары;
- басқарылатын құрылғылардың әрқайсысына арналған тапсырмалар:
  - зиянды БҚ жылдам іздеу;
  - жаңартулар жүктеп алу.

Егер сіз BYOL моделі бойынша лицензиялау нұсқасын таңдаған болсаңыз, онда бұлтты орта конфигурациясы Kaspersky Security Center-ді кілт файлы немесе белсендіру коды арқылы белсендіреді және кілт файлын немесе белсендіру кодын лицензиялар қоймасына орналастырады.

1-қадам. Бағдарламаны белсендіру тәсілін таңдау

AMI дайын кескіндерінің біріне жазылған болсаңыз (AWS Marketplace қолданбалар дүкенінде) немесе SKU қолдану үшін ай сайынғы есепті қолдансаңыз (Azure Marketplace дүкенінде), бұл қадам көрсетілмейді. Бұл жағдайда, шебер келесі қадамды бірден көрсетеді. Google Cloud үшін AMI дайын кескінін сатып ала алмайсыз.

BYOL схемасы бойынша Kaspersky Security Center лицензиялау нұсқасын таңдаған болсаңыз, шебер сізге бағдарламаны белсендіру тәсілін таңдауды ұсынады.

Kaspersky Security for Virtualization бағдарламасына немесе Kaspersky Hybrid Cloud Security бағдарламасына арналған белсендіру кодын (немесе кілт файлын) пайдаланып, бағдарламаны белсендіріңіз.

Бағдарламаны келесі жолдармен белсендіруге болады:

- Белсендіру кодын енгізу.

  Онлайн-белсендіру процесі іске қосылады. Бұл процесс барысында көрсетілген белсендіру коды тексеріледі, кілт файлы алынады және белсендіріледі.

- Кілт файлын көрсету.

  Бағдарлама кілт файлын тексереді және ішінде дұрыс ақпарат болса, оны белсендіреді немесе басқа кілт файлын көрсетуді ұсынады.

Kaspersky Security Center лицензиялық кілтті лицензиялар қоймасына орналастырады және оны басқарылатын құрылғыларға автоматты түрде таратылатын деп белгілейді.

Данаға Microsoft Windows "Қашықтағы жұмыс үстеліне қосылу" (Remote Desktop Connection) стандартты бағдарламасы немесе ұқсас бағдарлама арқылы қосылсаңыз, қашықтан қосылу сипаттарында сіз қосылатын физикалық құрылғының дискісін көрсетуіңіз керек. Осылайша, дананың физикалық құрылғыңыздағы файлдарға қатынасуын қамтамасыз ететін боласыз және кілт файлын таңдап, көрсете аласыз.

AMI ақылы кескінінде орналастырылған Kaspersky Security Center-пен жұмыс істеген кезде немесе қолдану үшін ай сайын шот ұсынып тұратын SKU қолданған кезде, лицензиялар қоймасына кілттер файлын немесе белсендіру кодтарын қосуға болмайды.

2-қадам. Бұлтты ортаны таңдау

Kaspersky Security Center орналастырылатын бұлтты ортаны таңдаңыз: AWS, Azure немесе Google Cloud.

3-қадам. Бұлтты ортадағы түпнұсқалық растама

AWS

AWS таңдасаңыз, қажетті құқықтары бар IAM рөлі бар екенін көрсетіңіз немесе Kaspersky Security Center-ге AWS IAM қатынас кілтін ұсыныңыз. IAM рөлі немесе AWS IAM қатынас кілті болмас, бұлттық сегменттерде сауалнама өткізу мүмкін емес.

Алдағыда бұлт бойынша сауалнама үшін қолданылатын келесі қосылым параметрлерін көрсетіңіз:

- **Қосылым атауы**

  Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

  Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

  Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

- **Use AWS IAM role**

  Басқару сервері AWS сервистерімен жұмыс істеуі үшін IAM рөлін жасаған болсаңыз, осы нұсқаны таңдаңыз.

- **AWS IAM пайдаланушы есептік жазбасын пайдалану**

  Сізде қажетті құқықтары бар IAM пайдаланушысының есептік жазбасы бар болса және сіз кілт идентификаторы мен құпия кілтті енгізе алсаңыз, осы нұсқаны таңдаңыз.

  - **Қатынас кілтінің идентификаторы**

    IAM қатынас кілті идентификаторы – әріптер мен сандар бірізділігі. IAM пайдаланушысы есептік жазбасын жасау кезінде кілттің идентификаторын алдыңыз.

    Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

  - **Құпия кілт**

    IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

    Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

    Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

Қосылым бағдарлама параметрлерінде сақталады. Бұлтты ортаны конфигурациялаудың көмегімен тек бір AWS IAM қатынас кілтін жасай аласыз. Кейінірек, сіз басқа бұлттық сегменттерді басқару үшін басқа қосылымдарды да көрсете аласыз.

Kaspersky Security Center құралдарымен даналарға бағдарламалар орнатқыңыз келсе, сіздің IAM рөліңіз (немесе есептік жазбасы сіз енгізген кілтке сәйкес келетін IAM пайдаланушысы) қажетті артықшылықтарға ие болуы қажет.

Azure

Azure таңдасаңыз, бұлттық сегменттерде сауалнама өткізу үшін келесі қосылым параметрлерін көрсетіңіз:

- **Қосылым атауы**

  Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

  Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

  Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

- **Azure бағдарламасының идентификаторы.**

  Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

  Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

- **Azure жазылым идентификаторы**

  Azure порталында жазылым жасадыңыз.

- **Azure бағдарлама құпиясөзі.**

  Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

- **Azure сақтау орнының есептік жазба атауы**

  Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

- **Azure сақтау орнының қатынас кілті**

  Сіз Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау есептік жазбасын жасаған кезде құпиясөз (кілт) алдыңыз.

  Кілт "Overview of the Azure storage account" бөлімінде, "Keys" бөлікшесінде қолжетімді.

Қосылым бағдарлама параметрлерінде сақталады.

Google Cloud

Google Cloud таңдасаңыз, бұлттық сегменттерде сауалнама өткізу үшін келесі қосылым параметрлерін көрсетіңіз:

- **Қосылым атауы**

  Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

  Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

  Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

- **Клиенттің электрондық поштасы**

  Клиенттің электрондық поштасы – бұл сіздің жобаңызды Google Cloud-қа тіркеу үшін пайдаланған электрондық пошта мекенжайы.

- **Жоба идентификаторы**

  Жоба идентификаторы – бұл Google Cloud жобасын тіркеу кезінде алынған идентификатор.

- **Жеке кілт**

  Жеке кілт – бұл жобаны Google Cloud-қа тіркеу кезінде жеке кілт ретінде алынған таңбалар бірізділігі. Қателерді болдырмау үшін осы бірізділікті көшіруге және қоюға болады.

Қосылым бағдарлама параметрлерінде сақталады.

4-қадам. Бұлтты ортамен синхрондау және кейінгі әрекеттерді анықтау

Бұл қадамда бұлттық сегменттерде сауалнама өткізу басталады және даналар үшін арнайы басқару тобы құрылады. Сауалнама кезінде табылған даналар осы топқа көшіріледі. Бұлттық сегменттерде сауалнама өткізу кестесі конфигурацияланады (әдепкі бойынша 5 минут сайын).

Сондай-ақ, **Бұлтпен синхрондау** автоматты түрде жылжыту ережесі жасалады. Бұлтты ортаны әрбір рет сканерлеген сайын, табылған виртуалды құрылғылар **Басқарылатын құрылғылар****Cloud** тобының ішіндегі тиісті ішкі топқа көшіріледі.

Бұлттық сегментпен синхрондау бетінде келесі параметрлерді белгілеуге болады:

- **Басқару тобының құрылымын бұлттық сегментпен синхрондау**

  Параметр қосулы болса, онда **Басқарылатын құрылғылар** тобында **Cloud** тобы автоматты түрде жасалып, бұлтты ортада құрылғыларды табу процесі іске қосылады. Бұлтты желіні әрбір рет сканерлеу кезінде табылған даналар мен виртуалды машиналар Cloud тобына көшіріледі. Бұл топтағы басқару ішкі топтарының құрылымы бұлттық сегменттің құрылымына сәйкес келеді (AWS-те қолжетімділік аймақтары мен орналастыру топтары құрылымда көрсетілмеген; Azure-да ішкі желілер құрылымда көрсетілмеген). Бұлтты ортада даналар ретінде анықталмаған құрылғылар **Тағайындалмаған құрылғылар** тобында болады. Мұндай топ құрылымы антивирустық бағдарламаларды топтық орнату тапсырмалары арқылы даналарға орнатуға және әртүрлі топтар үшін әртүрлі саясаттарды конфигурациялауға мүмкіндік береді.

  Параметр өшірулі болса, онда **Cloud** тобы да құрылады және бұлтты желідегі құрылғыларды анықтау процесі басталады, алайда топта бұлттық сегментінің құрылымына сәйкес келетін ішкі топтар жасалмайды. Табылған барлық даналар **Cloud** басқару тобында және бір тізімде көрсетіледі. Kaspersky Security Center-мен жұмыс істеу барысында сізге синхрондау қажет болса, онда сіз **Бұлтпен синхрондау** ережесінің сипаттарын өзгертіп, оны қолдана аласыз. Ережені қолдану Cloud тобы ішіндегі топтардың құрылымын бұлттық сегментіңіздің құрылымына сәйкес келетіндей етіп қайта реттейді.

  Әдепкі бойынша, параметр өшірулі.

- **Қорғауды жаю**

  Бұл параметр таңдалса, онда шебер қауіпсіздік бағдарламаларын даналарға орнату тапсырмасын жасайды. Шебердің жұмысы аяқталғаннан кейін, бұлттық сегменттеріңіздегі құрылғыларда қорғанысты орналастыру шебері автоматты түрде іске қосылады және сіз бұл құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орната аласыз.

  Kaspersky Security Center өз құралдарының көмегімен орналастыруды орындай алады. Amazon EC2 даналарына немесе Azure виртуалды машиналарына бағдарламаларды орнатуға құқығыңыз болмаса, **қашықтан орнату** тапсырмасын қолмен конфигурациялауға және қажетті құқықтары бар есептік жазбаны көрсетуге болады. Бұл жағдайда, қашықтан орнату тапсырмасы AWS API немесе Azure арқылы анықталған құрылғылар үшін жұмыс істемейді. Бұл тапсырма тек Active Directory сауалнамасы, Windows домендері немесе IP ауқымдары арқылы анықталған құрылғылар үшін ғана жұмыс істейді.

  Бұл параметр таңдалмаса, онда қорғанысты орналастыру шебері іске қосылмайды және қауіпсіздік бағдарламаларын даналарға орнату тапсырмалары жасалмайды. Бұл екі әрекетті де кейінірек қолмен жасауға болады.

Google Cloud-ты тек Kaspersky Security Center құралдарының көмегімен орналастыруға болады. Google Cloud-ты таңдасаңыз, **Қорғауды жаю** нұсқасы қолжетімді болмайды.

5-қадам. Бұлтты ортада Kaspersky Security Network конфигурациялау

Kaspersky Security Center жұмысы туралы ақпаратты Kaspersky Security Network білім базасына беру параметрлерін конфигурациялаңыз. Келесі нұсқалардың бірін таңдаңыз:

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын**

  Kaspersky Security Center және клиент құрылғыларында орнатылған басқарылатын бағдарламалар, олардың жұмысы туралы ақпаратты Kaspersky Security Network қызметіне автоматты режимде жіберетін болады. Kaspersky Security Network-пен ынтымақтастық, вирустар мен қауіптер туралы дерекқорды барынша жылдам жаңартуды қамтамасыз ете отырып, туындаған қауіпсіздік қауіптеріне жауап беру жылдамдығын арттырады.

- **Kaspersky Security Network пайдалану шарттарын қабылдамаймын**

  Kaspersky Security Center және басқарылатын бағдарламалар өз жұмысы туралы ақпаратты Kaspersky Security Network қызметіне жібермейді.

  Осы параметрді таңдасаңыз, Kaspersky Security Network қызметі өшіріледі.

Kaspersky компаниясы Kaspersky Security Network қызметіне қатысуды ұсынады.

6-қадам. Бұлтты ортада электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Виртуалды клиент құрылғыларында Kaspersky бағдарламалары жұмыс істеген кезде тіркелетін оқиғалар туралы хабарландыру тарату параметрлерін конфигурациялаңыз. Бұл параметрлер бағдарламалардың саясаттарында әдепкі бойынша мәндер ретінде пайдаланылады.

Kaspersky бағдарламаларының туындайтын оқиғалары туралы хабарландырулар таратылымын конфигурациялау үшін келесі параметрлер қолжетімді:

- **Алушылар (электрондық пошта мекенжайлары)**

  Бағдарлама хабарландыру жіберетін пайдаланушылардың электрондық пошта мекенжайлары. Бір не бірнеше мекенжайды енгізуге болады; бірнеше мекенжай енгізілсе, оларды нүктелі үтірмен бөліңіз.

- **SMTP серверлері**

  Ұйымыңыздың пошта серверлерінің мекенжайы немесе мекенжайлары.

  Бірнеше мекенжайды көрсетсеңіз, оларды үтірлі нүктемен бөліңіз. Келесі параметр мәндерін пайдалануыңызға болады:

  - IPv4 мекенжайы немесе IPv6 мекенжайы;
  - Windows желісіндегі құрылғының атауы (NetBIOS атауы);
  - SMTP сервері DNS атауы.

- **SMTP сервері порты**

  SMTP серверінің коммуникациялық портының нөмірі. Бірнеше SMTP серверін қолдансаңыз, олармен қосылым көрсетілген коммуникациялық порт арқылы орнатылады. Әдепкі бойынша 25-порт орнатылған.

- **ESMTP аутентификациясын пайдалану**

  ESMTP аутентификациясын қолдауды қосу. Жалаушаны қойғаннан кейін, ESMTP аутентификациясы параметрлерін **Пайдаланушы аты** және **Құпиясөз** өрістерінде көрсетуге болады. Әдепкі бойынша, жалауша алынып тасталған.

Пошта хабарландыруларын жіберудің орнатылған параметрлерін **Тексеру хабарын жіберу** түймесінің көмегімен тексере аласыз. Тексеру хабары **Алушылар (электрондық пошта мекенжайлары)** өрісінде көрсетілген мекенжайларға сәтті түрде жеткізілген болса, демек, параметрлер дұрыс конфигурацияланған.

7-қадам. Бұлтты ортада қорғаудың бастапқы конфигурациясын жасау

Бұл қадамда Kaspersky Security Center автоматты түрде саясаттар мен тапсырмаларды жасайды. **Қорғаудың бастапқы конфигурациясын жасау** терезесінде бағдарлама жасайтын саясаттар мен тапсырмалар тізімі көрсетіледі.

AWS бұлтты ортасында RDS дерекқорын қолдансаңыз, Басқару серверін сақтық көшірмелеу тапсырмасын жасау кезінде Kaspersky Security Center бағдарламасына IAM қатынас кілтін ұсынуыңыз керек. Бұл жағдайда, келесі өрістерді толтырыңыз:

- **S3 орнының атауы**

  Деректердің сақтық көшірмесі үшін жасалған S3 орнының атауы.

- **Қатынас кілтінің идентификаторы**

  Даналар қоймасындағы S3 орнымен жұмыс істеу үшін IAM пайдаланушысының есептік жазбасын жасаған кезде кілттің ID-ін (әріптер мен сандар бірізділігі) алдыңыз.

  Бұл өріс, S3 контейнеріне арналған RDS дерекқорын таңдаған кезде қолжетімді.

- **Құпия кілт**

  IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

  Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

  Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

Azure бұлтты ортасында Azure SQL дерекқорын қолдансаңыз, Басқару серверін сақтық көшірмелеу тапсырмасын жасау кезінде Azure SQL Server Kaspersky Security Center туралы ақпарат ұсынуыңыз керек. Бұл жағдайда, келесі өрістерді толтырыңыз:

- **Azure сақтау орнының есептік жазба атауы**

  Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

- **Azure жазылым идентификаторы**

  Azure порталында жазылым жасадыңыз.

- **Azure бағдарлама құпиясөзі.**

  Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

  Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

- **Azure бағдарламасының идентификаторы.**

  Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

  Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

- **Azure SQL сервері атауы**

  Көздің атауы мен тобы Azure SQL серверінің сипаттарында қолжетімді.

- **Azure SQL серверінің ресурстық тобы**

  Көздің атауы мен тобы Azure SQL серверінің сипаттарында қолжетімді.

- **Azure сақтау орнының қатынас кілті**

  "Access Keys" бөлімінде сақтаудың есептік жазбасы сипаттарында қолжетімді. Кез келген кілтті қолдана аласыз (key1 немесе key2).

Google Cloud-та Басқару серверін орналастыруды орындап жатсаңыз, сақтық көшірмелер сақталатын қалтаны таңдауыңыз керек. Жергілікті құрылғыда немесе виртуалды машина данасында қалтаны таңдаңыз.

Қорғаныстың минималды конфигурациясы үшін қажетті барлық саясаттар мен тапсырмалар жасалған кезде **Келесі** түймесі қолжетімді болады.

Егер тапсырмалар орындалуы тиісті құрылғы Басқару сервері желісінде көрінбесе, онда тапсырмалар тек құрылғы көрінген кезде ғана іске қосылады. EC2 немесе Azure виртуалды машинасын жасап жатсаңыз, онда дана немесе виртуалды машина Басқару серверіне көрінгенше біраз уақыт қажет болуы мүмкін. Желілік агент пен қауіпсіздік бағдарламалары барлық жаңа құрылғыларға барынша тезірек орнатылғанын қаласаңыз, онда **Бағдарламаны қашықтан орнату** тапсырмасы үшін Өткізіп алынған тапсырмаларды іске қосу параметрі қосулы екеніне **көз жеткізіңіз**. Әйтпесе, тапсырма кестеге сәйкес іске қосылмайынша, жасалған даналарға/виртуалды машиналарға Желілік агент пен қауіпсіздік бағдарламалары орнатылмайды.

8-қадам. Орнату барысында операциялық жүйені қайта іске қосу қажет болған кезде әрекетті таңдау (бұлтты орта үшін)

Бұған дейін **Қорғауды жаю** тармағын Қорғауды жаю болсаңыз, мақсатты құрылғының операциялық жүйесін қайта іске қосу қажет болса, сіз әрекетті таңдауыңыз керек болады. **Қорғауды жаю** параметрін таңдамасаңыз, бұл қадам өткізіп жіберіледі.

Бағдарламаларды құрылғыларға орнату барысында операциялық жүйені қайта іске қосу керек болса, даналарды қайта іске қосу қажет пе екенін таңдаңыз:

- **Құрылғыны қайта іске қоспау.**

  Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылмайды.

- **Құрылғыны қайта іске қосу**

  Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылады.

Қайта іске қосудың алдында даналарда бұғатталған сеанстардағы барлық бағдарламаларды мәжбүрлі түрде жапқыңыз келсе, **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы** жалаушасын қойыңыз. Жалауша қойылмаған болса, бұғаталған даналарда жұмыс істейтін барлық бағдарламаларды қолмен жабу керек.

9-қадам. Басқару сервері жаңартуларын алу

Бұл қадамда Басқару серверінің дұрыс жұмыс істеуі үшін қажетті жаңартуларды жүктеу процесі көрсетіледі. Шебердің соңғы терезесіне өту үшін жүктеудің аяқталуын күтпестен **Келесі** түймесін басуыңызға болады.

Шебер жұмысты аяқтайды.

Конфигурацияның сәтті орындалуын тексеру

Kaspersky Security Center 15.1 бағдарламасы бұлтты ортада дұрыс жұмыс істеу үшін конфигурацияланғанын тексеру үшін:

1. Kaspersky Security Center бағдарламасын іске қосыңыз және Басқару консолі арқылы Басқару серверіне қосыла алатыныңызға көз жеткізіңіз.
2. Консоль ағашында **Басқарылатын құрылғылар\Cloud** тармағын таңдаңыз.
3. **Басқарылатын құрылғылар\Cloud** тобы ішінде әрбір ішкі топқа кіре отырып, **Құрылғылар** қойыншасында әрбір ішкі топтың барлық құрылғылары көрсетілетініне көз жеткізіңіз.

   Егер құрылғылар көрсетілмесе, оларды табу үшін тиісті бұлттық сегментке қолмен сауалнама жүргізуге болады.
4. **Саясаттар** қойыншасында бағдарламалар үшін белсенді саясаттардың бар екеніне көз жеткізіңіз:
   - Kaspersky Security Center Желілік агенті
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Егер саясаттар тізімде болмаса, оларды қолмен жасауға болады.
5. **Тапсырмалар** қойыншасында келесі тапсырмалардың бар екеніне көз жеткізіңіз:
   - **Басқару сервері деректерінің сақтық көшірмесін жасау**
   - **Windows Server үшін жаңарту тапсырмасы**
   - **Басқару серверіне техникалық қызмет көрсету**
   - **Жаңартуларды Басқару серверінің қоймасына жүктеп алу**
   - **Осалдықтарды және қажетті жаңартуларды іздеу**
   - **Windows үшін қорғауды орнату**

- **Linux үшін қорғауды орнату**
- **Windows Server жылдам сауалнама тапсырмасы**
- **Жылдам сауалнама**
- **Linux үшін жаңартуды орнату**

Егер саясаттар тізімде болмаса, оларды қолмен жасауға болады.

Kaspersky Security Center 15.1 бағдарламасы бұлтты ортада дұрыс жұмыс істеу үшін конфигурацияланған.

Бұлтты құрылғылар тобы

Бұлтты құрылғыларды топтарға біріктіру арқылы басқаруға болады. Бастапқы конфигурациялау кезеңінде, Kaspersky Security Center әдепкі бойынша **Басқарылатын құрылғылар\Cloud** басқару тобын жасайды және желіде сауалнама өткізу кезінде анықталған бұлтты құрылғылар осы топқа салынады.

Синхрондауды конфигурациялау кезінде **Басқару тобының құрылымын бұлттық сегментпен синхрондау** жалаушасын қойған болсаңыз, онда осы басқару тобындағы ішкі топтар құрылымы бұлттық сегменттеріңіздің құрылымына сай келеді. (Алайда, қолжетімділік аймақтары мен орналастыру топтары AWS құрылымында ұсынылмаған, ішкі желілер Microsoft Azure құрылымында ұсынылмаған). Сауалнама өткізу кезінде анықталған топ ішіндегі бос ішкі топтар автоматты түрде жойылады.

Сондай-ақ, сіз барлық немесе кейбір құрылғыларды біріктіретін басқару топтарын өз бетіңізше жасай аласыз.

Басқарылатын құрылғылар\Cloud тобы әдепкі бойынша **Басқарылатын құрылғылар** тобынан саясаттар мен тапсырмаларды иеленеді. Тиісті саясат пен тапсырмалар параметрлерінің сипаттарында **Өңдеуге рұқсат етілген** жалаушалары қойылса, параметрлер конфигурацияларын өзгерте аласыз.

Бұлттық сегменттерде сауалнама өткізу

Желі құрылымы және оның құрамына кіретін құрылғылар туралы ақпаратты Басқару сервері AWS API, Azure API немесе Google API арқылы бұлттық сегменттерде тұрақты түрде сауалнама өткізу арқылы алады. Алынған ақпарат негізінде, Kaspersky Security Center бағдарламасы **Тағайындалмаған құрылғылар** және **Басқарылатын құрылғылар** қалталарының ішіндегісін жаңартады. Құрылғыларды басқару топтарына автоматты түрде жылжытуды конфигурациялаған болсаңыз, желіде анықталған құрылғылар басқару топтарының құрамына қосылады.

Басқару сервері бұлттық сегменттерде сауалнама жүргізе алуы үшін, IAM рөлі немесе IAM пайдаланушысы есептік жазбасы (AWS-те) қамтамасыз ететін құқықтар, қолданба идентификаторы және құпиясөз (Azure-да) немесе Google клиенті электрондық поштасының мекенжайы, Google жобасының идентификаторы және жеке кілт керек.

Қосылымдарды қосуға және жоюға, сондай-ақ әрбір бұлттық сегмент үшін сауалнама кестесін конфигурациялауға болады.

Бұлттық сегменттерде сауалнама өткізу үшін қосылымдарды қосу

Бұлттық сегменттерде сауалнама өткізу үшін қосылымды қолжетімділер тізіміне қосу үшін:

1. Консоль ағашында **Құрылғыны табу** → **Cloud** түйінін таңдаңыз.
2. Терезенің жұмыс аймағында **Сауалнама параметрлерін конфигурациялау** басыңыз.

   Бұлттық сегменттерде сауалнама өткізу үшін қолданылатын қосылымдар тізімі бар сипаттар терезесі ашылады.
3. **Қосу** түймесін басыңыз.

   Қосылым терезесі ашылады.
4. Алдағыда бұлттық сегменттерде сауалнама өткізу мақсатымен қолданылатын қосылым үшін бұлтты орта атауын көрсетіңіз:

   Бұлтты орта

   EC2 даналары (немесе виртуалды машиналар) орналасқан бұлтты орта Amazon Web Services (AWS), Microsoft Azure немесе Google Cloud болуы мүмкін.

   Егер сіз AWS таңдаған болсаңыз, келесі параметрлерді көрсетіңіз:

   - **Қосылым атауы**

     Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

     Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

     Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

   - **Use AWS IAM role**

     Басқару сервері AWS сервистерімен жұмыс істеуі үшін IAM рөлін жасаған болсаңыз, осы нұсқаны таңдаңыз.

   - **AWS IAM пайдаланушы есептік жазбасын пайдалану**

     Сізде қажетті құқықтары бар IAM пайдаланушысының есептік жазбасы бар болса және сіз кілт идентификаторы мен құпия кілтті енгізе алсаңыз, осы нұсқаны таңдаңыз.

     - **Қатынас кілтінің идентификаторы**

       IAM қатынас кілті идентификаторы – әріптер мен сандар бірізділігі. IAM пайдаланушысы есептік жазбасын жасау кезінде кілттің идентификаторын алдыңыз.

       Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

     - **Құпия кілт**

       IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

       Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

Бұлтты ортаны конфигурациялау шебері тек бір ғана AWS IAM қатынас кілтін көрсетуге мүмкіндік береді. Кейінірек, сіз басқа бұлттық сегменттерді басқару үшін басқа қосылымдарды да көрсете аласыз.

Егер сіз Azure таңдаған болсаңыз, келесі параметрлерді көрсетіңіз:

- **Қосылым атауы**

  Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

  Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

  Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

- **Azure бағдарламасының идентификаторы.**

  Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

  Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

- **Azure жазылым идентификаторы**

  Azure порталында жазылым жасадыңыз.

- **Azure бағдарлама құпиясөзі.**

  Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

  Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

- **Azure сақтау орнының есептік жазба атауы**

  Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

- **Azure сақтау орнының қатынас кілті**

  Сіз Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау есептік жазбасын жасаған кезде құпиясөз (кілт) алдыңыз.

  Кілт "Overview of the Azure storage account" бөлімінде, "Keys" бөлікшесінде қолжетімді.

Егер сіз Google Cloud таңдаған болсаңыз, келесі параметрлерді көрсетіңіз:

- **Қосылым атауы**

  Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

  Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

  Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

- **Клиенттің электрондық поштасы**

  Клиенттің электрондық поштасы – бұл сіздің жобаңызды Google Cloud-қа тіркеу үшін пайдаланған электрондық пошта мекенжайы.

- **Жоба идентификаторы**

  Жоба идентификаторы – бұл Google Cloud жобасын тіркеу кезінде алынған идентификатор.

- **Жеке кілт**

  Жеке кілт – бұл жобаны Google Cloud-қа тіркеу кезінде жеке кілт ретінде алынған таңбалар бірізділігі. Қателерді болдырмау үшін осы бірізділікті көшіруге және қоюға болады.

5. Қаласаңыз, **Сауалнама кестесін орнату** тармағын таңдап, әдепкі бойынша белгіленген параметрлерді өзгертіңіз.

Қосылым бағдарлама параметрлерінде сақталады.

Жаңа бұлттық сегментте бірінші сауалнама өткізгеннен кейін, **Басқарылатын құрылғылар****Cloud** басқару тобында осы сегментке сай келетін ішкі топ пайда болады.

Дұрыс емес есептік деректерді көрсеткен болсаңыз, онда бұлттық сегменттерде сауалнама өткізу кезінде даналар табылмайды, ал жаңа ішкі топ басқару **Басқарылатын құрылғылар****Cloud** тобында көрсетілмейді.

Бұлттық сегменттерде сауалнама өткізу үшін қосылымдарды жою

Егер сізге енді бұлттық сегментте сауалнама жүргізудің қажеті болмаса, қолжетімді тізімнен сол сегментке сәйкес келетін қосылымды жоя аласыз. Сондай-ақ, мысалы, бұлттық сегменттерде сауалнама өткізу құқықтары басқа кілті бар басқа AWS IAM пайдаланушысына ауысса, қосылымды жоюға болады.

Қосылымды жою үшін:

1. Консоль ағашында **Құрылғыны табу** → **Cloud** түйінін таңдаңыз.
2. Терезенің жұмыс аймағында **Сауалнама параметрлерін конфигурациялау** таңдаңыз.

   Бұлттық сегменттерде сауалнама өткізу үшін қолданылатын қосылымдар тізімі бар терезе пайда болады.
3. Жойғыңыз келетін қосылымды бөлектеңіз және терезенің оң жағындағы **Жою** түймесін басыңыз.
4. Пайда болған терезеде таңдауыңызды растау үшін **OK** түймесін басыңыз.

Егер сіз қосылымды қолжетімділер тізімінен алып тастасаңыз, онда тиісті сегменттердің ішіндегі құрылғылар тиісті басқару топтарынан автоматты түрде жойылады.

Сауалнама кестесін конфигурациялау

Бұлттық сегменттерде сауалнама өткізу кесте бойынша орындалады. Сіз сауалнама жүргізілетін жиілікті орната аласыз.

Бұлтты ортаны конфигурациялау шеберінің параметрлерінде сауалнама өткізу жиілігі автоматты түрде орнатылады – 5 минутта бір рет. Сіз бұл мәнді кез келген уақытта өзгерте аласыз және басқа кестені белгілей аласыз. Сауалнаманы 5 минутта бір реттен жиі жүргізу ұсынылмайды, себебі бұл API жұмысында қателерге әкелуі мүмкін.

Бұлттық сегменттерде сауалнама өткізу кестесін конфигурациялау үшін:

1. Консоль ағашында **Құрылғыны табу** → **Cloud** түйінін таңдаңыз.
2. Жұмыс аймағында **Сауалнама параметрлерін конфигурациялау** басыңыз.

   Нысан сипаттары терезесі ашылады.
3. Тізімде қажетті қосылымды таңдап, **Сипаттар** түймесін басыңыз.

   Қосылым сипаттары терезесі ашылады.
4. Сипаттар терезесінде **Сауалнама кестесін орнату** сілтемесі бойынша өтіңіз.

   Кесте терезесі ашылады.
5. Келесі параметрлерді конфигурациялаңыз:

   - **Кесте бойынша іске қосу**

     Сауалнама кестесінің нұсқалары:

     - **N күн сайын**

       Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

       Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

     - **N минут сайын**

       Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

       Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

     - **Апта күндері бойынша**

       Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

       Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

     - **Ай сайын, таңдалған апталардың көрсетілген күндері**

       Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

       Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

   - **Өткізіп алынған тапсырмаларды іске қосу**

     Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

     Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

     Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

Әдепкі бойынша, параметр қосулы.

6. Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

Сауалнама кестесі конфигурацияланған және сақталған.

Бағдарламаларды бұлтты ортадағы құрылғыларға орнату

Бұлтты ортадағы құрылғыларға келесі Kaspersky бағдарламаларын орнатуға болады: Kaspersky Security for Windows Server (Windows операциялық жүйесі бар құрылғылар үшін) және Kaspersky Endpoint Security for Linux (Linux операциялық жүйесі бар құрылғылар үшін).

Қорғанысты орнатқыңыз келетін клиент құрылғылары, Kaspersky Security Center-дің бұлтты ортада жұмыс істеуі үшін қойылған талаптарға сай келуі тиіс. AWS даналарына, Microsoft Azure виртуалды машиналарына немесе Google виртуалды машиналарының даналарына бағдарламаларды орнату үшін ағымдағы лицензияңыз болуы тиіс.

Kaspersky Security Center 15.1 келесі сценарийлерді қолдайды:

- Клиент құрылғысы API көмегімен анықталды; орнату да API арқылы орындалады. Бұл сценарийге AWS және Azure бұлтты ортасы үшін қолдау көрсетіледі.
- Клиент құрылғысы Active Directory, Windows домендері немесе IP ауқымдары сауалнамасы арқылы анықталады; орнату Kaspersky Security Center арқылы жүзеге асырылады.
- Клиент құрылғысы Google API көмегімен анықталды; орнату Kaspersky Security Center арқылы орындалады. Бұл сценарийге тек Google Cloud үшін қолдау көрсетіледі.

Бағдарлама орнатудың басқа тәсілдеріне қолдау көрсетілмейді.

Бағдарламаларды виртуалды құрылғыларға орнату үші орнату пакеттерін қолданыңыз.

Бағдарламаны AWS API немесе Azure API арқылы даналарға қашықтан орнату тапсырмасын жасау үшін:

1. Консоль ағашында **Тапсырмалар** қалтасын таңдаңыз.
2. **Жаңа тапсырма** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. **Тапсырма түрін таңдау** терезесінде **Бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.
4. **Құрылғыларды таңдау** терезесінде **Басқарылатын құрылғылар\Cloud** тобындағы қажетті құрылғыларды таңдаңыз.
5. Бағдарлама орнатқыңыз келетін құрылғыларға әлі Желілік агент орнатылмаған болса, **Тапсырманы іске қосу үшін есептік жазбаны таңдау** бетінде **Есептік жазба қажет (Желілік агент пайдаланылмайды)** тармағын таңдап, терезенің оң жағында **Қосу** түймесін басыңыз. Пайда болған мәзірде келесіні таңдаңыз:

   - **Бұлт есептік жазбасы**

     Бағдарламаларды AWS ортасындағы даналарға орнатқыңыз келсе және қажетті құқықтары бар AWS IAM қатынас кілтін алғыңыз келсе, бірақ IAM рөліне ие болғыңыз келмесе, осы параметрді таңдаңыз. Сондай-ақ, бағдарламаларды Azure ортасындағы құрылғыларға орнатқыңыз келсе, осы параметрді таңдаңыз.

Пайда болған терезеде Kaspersky Security Center-ге бағдарламаларды өзіңізге қажетті құрылғыларға орнатуға құқық беретін есептік деректерді ұсыныңыз.

AWS немесе Azure бұлтты ортасын таңдаңыз.

Есептік жазба атауы өрісінде осы есептік деректердің атауын енгізіңіз. Осы атау, тапсырманы іске қосу үшін есептік жазбалар тізімінде көрсетіледі.

AWS таңдаған болсаңыз, **қатынас кілті ID** және **Құпия кілт** өрістерінде бағдарламаларды көрсетілген құрылғыларда орнатуға құқығы бар IAM пайдаланушысы есептік деректерін енгізіңіз.

Azure таңдаған болсаңыз, **Azure жазылым идентификаторы** және **Azure бағдарлама құпиясөзі** өрістерінде, бағдарламаларды көрсетілген құрылғыларда орнатуға құқығы бар Azure есептік жазбасының деректерін енгізіңіз.

Дұрыс емес есептік деректерді көрсетсеңіз, бағдарламаларды қашықтан орнату тапсырмасы жоспарланған құрылғыларда қатемен аяқталады.

- **Есептік жазба**

  Windows операциялық жүйесі бар даналар үшін, бағдарламаны AWS немесе Azure API құралдарының көмегімен орнатпасаңыз, осы параметрді таңдаңыз. Бұл жағдайда, сіздің бұлттық сегментіңіздегі құрылғылар қажетті шарттарға сай келетіндігіне көз жеткізіңіз. Kaspersky Security Center, бағдарламаларды AWS API немесе Azure API қолданбай өз құралдарымен орнатады.

  Дұрыс емес деректерді көрсетсеңіз, бағдарламаларды қашықтан орнату тапсырмасы жоспарланған құрылғыларда қатемен аяқталады.

- **IAM рөлі**

  Бағдарламаларды AWS айналасындағы даналарға орнатқыңыз келсе және қажетті құқықтары бар IAM рөліне ие болғыңыз келсе, осы параметрді таңдаңыз.

  Осы параметрді таңдасаңыз, қажетті құқықтары бар IAM рөліңіз болмайды және бағдарламаларды қашықтан орнату тапсырмасы жоспарланған құрылғыларда қатемен аяқталады.

- **SSH сертификаты**

  Linux операциялық жүйесі бар даналар үшін, бағдарламаларды AWS API немесе Azure API құралдары көмегімен орнатпасаңыз, осы параметрді таңдаңыз. Бұл жағдайда, сіздің бұлттық сегментіңіздегі құрылғылар қажетті шарттарға сай келетіндігіне көз жеткізіңіз. Kaspersky Security Center, бағдарламаларды AWS API немесе Azure API қолданбай өз құралдарымен орнатады.

  SSH сертификатының жабық кілтін көрсету үшін, оны ssh-keygen утилитасы көмегімен генерациялай аласыз. Назар аударыңыз, Kaspersky Security Center, PEM жабық кілттері пішімін қолдайды, бірақ ssh-keygen утилитасы әдепкі бойынша OPENSSH пішіміндегі SSH кілттерін генерациялайды. OPENSSH пішімін Kaspersky Security Center қолдайды. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін `-m PEM` параметрін ssh-keygen пәрменіне қосыңыз. Мысалы:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<пайдаланушының электрондық поштасы>"
  ```

Әрбір рет **Қосу** түймесін басу арқылы бірнеше есептік деректерді ұсына аласыз. Бұлттық сегменттер әртүрлі есептік деректерді талап етсе, барлық сегменттер үшін есептік деректерді көрсетіңіз.

Бағдарламаны қашықтан орнату тапсырмасы **Тапсырмалар** қалтасының жұмыс аймағындағы тапсырмалар тізімінде пайда болады.

Microsoft Azure-да қауіпсіздік бағдарламаларын виртуалды машинаға қашықтан орнату, осы виртуалды машинада орнатылған скрипттердің конфигурацияланатын кеңейтімінің жойылуына әкелуі мүмкін.

Бұлтты құрылғылардың сипаттарын қарап шығу

Бұлтты құрылғының сипаттарын қарап шығу үшін:

1. Консоль ағашындағі **Құрылғыны табу** → **Cloud** қалтасында өзіңізге қажетті дана орналасқан топқа сай келетін қалтаны таңдаңыз.

   Өзіңізге қажетті виртуалды құрылғының қандай топта екенін білмесеңіз, іздеуді қолданыңыз:

   a. **Басқарылатын құрылғылар** → **Cloud** түйінінде тінтуірдің оң жақ түймесін басып, мәнмәтіндік мәзірден **Іздеу** тармағын таңдаңыз.

   b. Пайда болған терезеде іздеуді орындаңыз.

      Енгізілген өлшемшарттарға сай келетін құрылғы бар болса, оның атауы мен ол туралы ақпарат терезенің астында көрсетілетін болады.

2. Қажетті түйіннің атауында тінтуірдің оң жақ түймесін басыңыз. Мәнмәтіндік мәзірден **Сипаттар** тармағын таңдаңыз.

   Пайда болған терезеде нысан сипаттары көрсетіледі.

   Жүйе туралы ақпарат → **Жалпы жүйе ақпараты** бөлімінде бұлтты ортадағы құрылғыларға тән параметрлер бар:

   - **Құрылғы API арқылы табылды** (**AWS**, **Azure** немесе **Google Cloud**; құрылғыны API құралдарының көмегімен табу мүмкін болмаса, **Жоқ** мәні көрсетіледі).
   - **Бұлтты аймақ**.
   - **Cloud VPC** (тек AWS және Google Cloud құрылғылары үшін ғана).
   - **Бұлтты қолжетімділік аймағы** (тек AWS және Google Cloud құрылғылары үшін ғана).
   - **Бұлтты қосалқы желісі**.
   - **Бұлтты орналастыру тобы** (бұл құрылғы, дана орналастыру тобына тиесілі болса көрсетіледі; әйтпесе, сипат көрсетілмейді).

Осы ақпаратты CSV немесе TXT пішіміндегі файлға экспорттау үшін, **Файлға экспорттау** түймесін басыңыз.

Бұлтпен синхрондау

Бұлтты ортаны конфигурациялау кезінде Бұлтты ортамен синхрондау ережесі автоматты түрде жасалады. Бұл ереже әрбір сауалнамада табылған даналарды **Тағайындалмаған құрылғылар** тобынан **Басқарылатын құрылғылар\Cloud** тобына автоматты түрде көшіруге мүмкіндік береді, осылайша даналар орталықтан басқару үшін қолжетімді болады. Әдепкі бойынша, ереже жасалғаннан кейін қосулы болады. Сіз ережені қалған уақытта өшіре аласыз, өзгерте аласыз немесе қолдана аласыз.

Бұлтпен синхрондау ережесінің сипаттарын өзгерту және/немесе ережені қолдану үшін:

1. Консоль ағашындағі **Құрылғыны табу** түйінің атауында тінтуірдің оң жақ түймесін басыңыз.
2. Мәнмәтіндік мәзірден **Сипаттар** тармағын таңдаңыз.
3. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Құрылғыларды жылжыту** бөлімін таңдаңыз.
4. Құрылғыны жылжыту ережелері тізімінде **Бұлтпен синхрондау** тармағын таңдап, терезенің астындағы **Сипаттар** түймесін басыңыз.

   Ереже сипаттары терезесі ашылады.
5. Қажет болса, **Бұлттық сегменттер** параметрлері блогында келесі параметрлерді көрсетіңіз:

   - **Құрылғы бұлттық сегментте орналасқан**

     Ереже тек таңдалған бұлттық сегментте орналасқан құрылғыларда ғана қолданылады. Әйтпесе, ереже барлық анықталған құрылғыларда қолданылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

     - **Қосалқы нысандарды қосу**

       Ереже таңдалған сегменттегі барлық құрылғылар үшін және оның барлық салынған бұлттық бөлімдерінде орындалады. Әйтпесе, ереже түбірлік сегменттегі құрылғылар үшін қолданылады.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **Құрылғыларды кірістірілген нысандардан сәйкес қосалқы топтарға жылжыту**

       Параметр қосулы болса, онда құрылғылар салынған нысандардан олардың құрылымына сай келетін ішкі топтарға көшіріледі.

       Параметр қосулы болса, онда құрылғылар салынған нысандардан Cloud ішкі тобының түбіріне көшіріліп, ішкі топтарға бөлінбейді.

       Әдепкі бойынша, параметр қосулы.

       - **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау**

         Жалауша қойылған болса, онда **Басқарылатын құрылғылар\Cloud** топтары құрылымында құрылғы орналасқан бөлімге сай келетін ішкі топ болмаса, онда Kaspersky Security Center осындай ішкі топты құрады. Мысалы, құрылғыларды анықтау барысында жаңа ішкі желі анықталған болса, онда **Басқарылатын құрылғылар\Cloud** тобында осындай атауы бар жаңа топ құрылатын болады.

         Параметр өшірулі болса, онда Kaspersky Security Center ішкі топтарды құрмайды. Мысалы, жаңа ішкі желі желіде сауалнама жүргізу кезінде анықталған болса, онда осындай атауы бар жаңа топ **Басқарылатын құрылғылар\Cloud** тобының астында құрылып, осы ішкі желідегі құрылғылар **Басқарылатын құрылғылар\Cloud** тобына көшірілмейді.

         Әдепкі бойынша, параметр қосулы.

       - **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою**

         Параметр қосулы болса, онда бағдарлама Cloud тобынан ешқандай бұлтты нысандарға сай келмейтін ішкі топтарды жоятын болады.

         Параметр өшірулі болса, онда бұлтты нысандарға сай келмейтін ішкі топтар сақталмайды.

         Әдепкі бойынша, параметр қосулы.

Бұлтты ортаны конфигурациялау кезеңінде **Бұлтпен синхрондау** параметрін қосқан болсаңыз, онда Бұлтпен синхрондау ережесі **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау** және **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою** жалаушаларын қою арқылы жасалады.

Бұлтпен синхрондау параметрін қоспаған болсаңыз, онда ереже өшірулі параметрмен бірге жасалатын болады. Kaspersky Security Center-мен жұмыс істеу барысында **Басқарылатын құрылғылар\Cloud** ішкі тобы ішіндегі ішкі топтар құрылымы бұлттық сегменттер құрылымына сай келуін қаласаңыз, ереженің сипаттарында **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау** және **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою** параметрлерін қосыңыз.

6. **Құрылғы API арқылы табылды** ашылмалы тізімінде мәнді таңдаңыз:
   - **AWS**. Құрылғы AWS API арқылы табылды, яғни құрылғы AWS бұлтты ортасында орналасқан.
   - **Azure**. Құрылғы Azure API арқылы табылды, яғни құрылғы Azure бұлтты ортасында орналасқан.
   - **Google Cloud.** Құрылғы Google API арқылы табылды, яғни құрылғының Google Cloud ортасында орналасқаны анық.
   - **Жоқ**. Құрылғыны AWS, Azure немесе Google API пайдалану арқылы анықтау мүмкін емес, яғни ол бұлттық ортадан тыс немесе бұлттық ортада, бірақ оны API арқылы анықтау мүмкін емес.
7. **Көрсетілмеген**. Бұл шарт қолданылмайды. Қажет болса, басқа бөлімдерде ереженің басқа да сипаттарын конфигурациялаңыз.
8. Қажет болса, терезенің астындағы **Мәжбүрлі түрде** түймесін басып, ережені қолданыңыз.

   Ережені орындау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз. Шебердің жұмысы аяқталғаннан кейін, ереже іске қосылып, **Басқарылатын құрылғылар\Cloud** ішкі тобының ішіндегі топтар құрылымы сіздің бұлттық сегменттеріңіздің құрылымына сай келетін болады.
9. **ОК** түймесін басыңыз.

Параметрлер конфигурацияланған және сақталған.

Cloud-пен синхрондау ережесін өшіру үшін:

1. Консоль ағашындағы **Құрылғыны табу** түйінің атауында тінтуірдің оң жақ түймесін басыңыз.
2. Мәнмәтіндік мәзірден **Сипаттар** тармағын таңдаңыз.
3. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Құрылғыларды жылжыту** бөлімін таңдаңыз.
4. Құрылғыларды жылжыту ережелері тізімінде **Бұлтпен синхрондау** параметрін өшіріп, **ОК** түймесін басыңыз.

Ереже өшіріліп, енді қолданылмайды.

Kaspersky Security Center бағдарламасының Yandex.Cloud ортасындағы жұмыс схемасы

Kaspersky Security Center бағдарламасын Yandex.Cloud бұлтты ортасында орналастыра аласыз. Тек пайдалану фактісі бойынша төлем режимі қолжетімді; бұлтты дерекқорларға қолдау көрсетілмейді.

Yandex.Cloud бұлтты ортасында кезесі қауіпсіздік бағдарламаларын орналастыру тәсілдері қолжетімді:

- Kaspersky Security Center меншікті құралдары көмегімен, яғни *Қашықтан орнату* тапсырмасын қолдану арқылы (қауіпсіздік бағдарламаларын орналастыру Басқару сервері мен қорғалатын виртуалды машиналар желінің бір сегментінде болған жағдайда ғана мүмкін болады)

- Орналастыру скриптілері арқылы

Kaspersky Security Center бағдарламасын Yandex.Cloud бұлтты ортасында орналастыру үшін сізде Yandex.Cloud есептік жазбасы болуы керек. Осы есептік жазбаға marketplace.meteringAgent рұқсатын беріп, осы есептік жазбаны виртуалды машинамен байланыстыруыңыз керек (толық ақпарат https://cloud.yandex.ru бетінде).

Қолданба

Бұл бөлімде Kaspersky Security Center пайдалану туралы анықтамалық және кеңейтілген ақпарат бар.

Кеңейтілген мүмкіндіктер

Бұл бөлімде құрылғылардағы бағдарламаларды орталықтандырылған түрде басқару мүмкіндіктерін кеңейтуге арналған Kaspersky Security Center бағдарламасының бірқатар қосымша функциялары қарастырылады.

Kaspersky Security Center жұмысын автоматтандыру. klakaut утилитасы

Сіз Kaspersky Security Center жұмысын klakaut утилитасының көмегімен автоматтандыра аласыз. klakaut утилитасы және оған арналған анықтамалық жүйе Kaspersky Security Center орнату қалтасында орналасқан.

Реттелмелі құралдармен жұмыс

Kaspersky Security Center бағдарламасы *сыртқы құралдар* (бұдан әрі – *құралдар*) – **Реттелмелі құралдар** контекстік мәзірі тобы арқылы Басқару консолінен клиент құрылғысы үшін шақырылатын бағдарламалар тізімін құрастыруға мүмкіндік береді. Әрбір құрал үшін тізімнен жеке мәзір пәрмені жасалады және оның көмегімен Басқару консолі құралға сәйкес келетін бағдарламаны іске қосады.

Бағдарлама әкімшінің жұмыс станциясында іске қосылады. Пәрмен жолының аргументтері ретінде бағдарлама қашықтағы клиент құрылғысының атрибуттарын қабылдай алады (NetBIOS атауы, DNS атауы, IP мекенжайы). Қашықтағы құрылғыға қосылу туннельді қосылым арқылы жүзеге асырылуы мүмкін.

Әрбір клиент құрылғысы үшін әдепкі бойынша сыртқы құралдар тізімінде келесі сервистік бағдарламалар бар:

- **Қашықтан диагностикалау** – Kaspersky Security Center қашықтан диагностикалау утилитасы.

- **Қашықтағы жұмыс үстелі** – Microsoft Windows "Қашықтағы жұмыс үстеліне қосылу орындалуда" стандартты құрамдасы.

- **Компьютерді басқару** – Microsoft Windows стандартты құрамдасы.

Сыртқы құралдарды қосу немесе жою және олардың параметрлерін өзгерту үшін,

Таңдалған құрылғының контекстік мәзірінде **Реттелмелі құралдар** → **Реттелмелі құралдарды конфигурациялау** тармағын таңдаңыз.

Реттелмелі құралдар терезесі ашылады. Бұл терезеде **Қосу** және **Өзгерту** түймелері арқылы сыртқы құралдарды қосуға немесе олардың параметрлерін өзгертуге болады. Сыртқы құралдарды жою үшін қызыл кірес белгішесі (❌) бар жою түймесін басыңыз.

Желілік агенттің дискісін клондау режимі

"Эталонды" құрылғының қатты дискісін клондау, бағдарламалық жасақтаманы жаңа құрылғыларға орнатудың кеңінен таралған тәсілі болып табылады. Клондау барысында "эталонды" құрылғының қатты дискісіндегі Желілік агент әдеттегі режимде жұмыс істесе, келесі мәселе туындайды:

Желілік агенті бар дискінің эталонды бейнесін жаңа құрылғыларға енгізгеннен кейін, бұл құрылғылар Басқару консолінде бір белгішемен көрсетіледі. Мәселе, клондау кезінде жаңа құрылғыларда Басқару серверіне құрылғыны Басқару консолінде белгішемен байланыстыруға мүмкіндік беретін бірдей ішкі деректер сақталатындықтан туындайды.

Клондағаннан кейін Басқару консолінде жаңа құрылғыларды дұрыс көрсетпеумен байланысты мәселелерді болдырмау үшін арнайы *Желілік агент дискісін клондау режимі* көмектеседі. Бағдарламалық жасақтаманы жаңа құрылғыларға дискіні клондау арқылы енгізіп жатсаңыз (Желілік агентпен бірге), осы режимді қолданыңыз.

Дискіні клондау режимінде, Желілік агент жұмыс істеп тұрғанымен, Басқару серверіне қосылмайды. Клондау режимінен шығу кезінде, Желілік агент ішкі деректерді жояды, олардың болуы себебінен Басқару сервері бірнеше құрылғыны Басқару консолінде бір белгішемен байланыстырады. "Эталонды" құрылғының бейнесін клондап болғаннан кейін, жаңа құрылғылар Басқару консолінде қалыпты түрде (бөлек белгішелермен) көрсетіледі.

Желілік агент дискісін клондау режимін қолдану сценарийі

1. Әкімші Желілік агентті "эталонды" құрылғыда орнатады.
2. Әкімші Желілік агенттің Басқару серверіне қосылуын klnagchk утилитасы арқылы тексереді.
3. Әкімші Желілік агент дискісін клондау режимін қосады.
4. Әкімші құрылғыға бағдарламалық жасақтаманы, патчтарды орнатады және құрылғыны қайта жүктеудің кез келген санын орындайды.
5. Әкімші "эталонды" құрылғының қатты дискісін құрылғылардың кез келген санына клондайды.
6. Әрбір клондалған көшірме үшін келесі шарттар орындалуы тиіс:
   a. құрылғының атауы өзгертілген;
   b. құрылғы қайта жүктелген;
   c. дискіні клондау режимі өшірулі.

Дискіні klmover утилитасы көмегімен клондау режимін қосу және өшіру

Желілік агент дискісін клондау режимін қосу немесе өшіру үшін:

1. Клондау қажет болған Желілік агенті орнатылған құрылғыда klmover утилитасын іске қосыңыз.

   klmover утилитасы Желілік агентті орнату қалтасында орналасқан.

2. Дискіні клондау режимін қосу үшін Windows пәрмен қабықшасына келесі пәрменді енгізіңіз:

   ```
   klmover -cloningmode 1
   ```

   Желілік агент дискіні клондау режиміне ауысады.

3. Дискіні клондау режимінің ағымдағы күйін сұрау үшін пәрмен жолына келесі пәрменді енгізіңіз:

   ```
   klmover -cloningmode
   ```

   Нәтижесінде, утилитаның терезесінде дискіні клондау режимінің қосулы немесе өшірулі екені туралы ақпарат көрсетіледі.

4. Дискіні клондау режимін өшіру үшін утилитаның пәрмен жолына келесі пәрменді енгізіңіз:

   ```
   klmover -cloningmode 0
   ```

Операциялық жүйенің бейнесін жасау үшін Желілік агенті орнатылған эталонды құрылғыны дайындау

Сіз Желілік агент орнатылған эталондық құрылғының операциялық жүйесінің кескінін жасай аласыз, содан кейін кескінді желілік құрылғыларға орналастыра аласыз. Бұл жағдайда, сіз Желілік агент әлі іске қосылмаған эталондық құрылғының операциялық жүйесінің кескінін жасайсыз. Егер сіз операциялық жүйенің кескінін жасамас бұрын эталондық құрылғыда Желілік агентті іске қоссаңыз, эталондық құрылғының операциялық жүйесінің кескінінен орналастырылған құрылғылардың Басқару серверін анықтау қиынға соғады.

Операциялық жүйенің кескінін жасау мақсатымен эталондық құрылғыны дайындау үшін:

1. Windows операциялық жүйесі эталондық құрылғыға орнатылғанына көз жеткізіңіз, сонымен қатар осы құрылғыда қажет басқа бағдарламалық жасақтаманы орнатыңыз.

2. Эталондық құрылғыда, Windows желілік қосылым параметрлерінде эталондық құрылғыны Kaspersky Security Center орнатылған желіден ажыратыңыз.

3. Эталондық құрылғыда setup.exe файлын пайдаланып, Желілік агентті жергілікті түрде орнатуды іске қосыңыз.

   Kaspersky Security Center Желілік агентін орнату шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

4. Шебердің **Басқару сервері** бетінде Басқару серверінің IP мекенжайын көрсетіңіз.

   Басқару серверінің нақты мекенжайын білмесеңіз, localhost енгізіңіз. `-address` кілті бар klmover утилитасын қолдана отырып, IP мекенжайын кейінірек өзгерте аласыз.

5. Шебердің **Бағдарламаны іске қосу** бетінде **Бағдарламаны орнату барысында іске қосу** параметрін өшіріңіз.

6. Желілік агент орнатылғаннан кейін, операциялық жүйенің кескінін жасамас бұрын құрылғыны қайта іске қоспаңыз.

   Егер сіз құрылғыны қайта іске қоссаңыз, операциялық жүйенің кескінін жасау үшін эталондық құрылғыны жасаудың бүкіл процесін қайталауыңыз керек.

7. Эталондық құрылғыда, пәрмен жолында sysprep утилитасын іске қосып, келесі пәрменді орындаңыз: `sysprep.exe /generalize /oobe /shutdown`.

Эталондық құрылғы операциялық жүйе кескінін жасауға дайын.

Файл тұтастығын басқару құрамдасынан хабар алу параметрлерін конфигурациялау

Kaspersky Security for Windows Server немесе Kaspersky Hybrid Cloud Security for Virtualization Жеңіл агент сияқты басқарылатын бағдарламалар Kaspersky Security Center-ге Файл тұтастығын басқару құрамдасынан хабарлар жібереді. Сонымен қатар, Kaspersky Security Center жүйелердің критикалық маңызды аймақтарының (мысалы, веб-серверлер, банкоматтар) өзгермейтіндігін бақылауға және осындай жүйелердің тұтастығының бұзылуына жедел ден қоюға мүмкіндік береді. Ол үшін Файл тұтастығын басқару құрамдасынан хабарлар алуға қолдау көрсету іске асырылған. Файл тұтастығын басқару құрамдасы құрылғының файлдық жүйесін ғана емес, сонымен қатар тізімдеме тарамдарын, желілік экранның күйін және қосылған жабдықтың күйін бақылауға мүмкіндік береді.

Kaspersky Security for Windows Server немесе Kaspersky Security for Virtualization Жеңіл агент бағдарламаларын пайдаланбай, Файл тұтастығын басқару құрамдасынан хабарлар алу үшін Kaspersky Security Center конфигурациясын орындау қажет.

Файл тұтастығын басқару құрамдасынан хабарлар алу параметрлерін конфигурациялау үшін:

1. Басқару сервері орнатылған құрылғының жүйелік тізімдемесін, мысалы, жергілікті түрде **Бастау** → **Орындау** мәзіріндегі regedit пәрменінің көмегімен ашыңыз.

2. Келесі бөлімге өтіңіз:

   - 32 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - 64 разрядты жүйе үшін:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Кілттер жасаңыз:

   - Өңделген оқиғалар санын санау уақыт аралығын көрсету үшін KLSRV_EVP_FIM_PERIOD_SEC кілтін жасаңыз. Келесі параметрлерді белгілеңіз:

     a. Кілт атауын KLSRV_EVP_FIM_PERIOD_SEC деп көрсетіңіз.

     b. Кілт түрін DWORD деп көрсетіңіз.

     c. 43 200-172 800 секунд уақыт аралығы үшін мәндер ауқымын көрсетіңіз. Әдепкісінше уақыт аралығы — 86 400 секунд.

- Көрсетілген уақыт аралығында қабылданатын оқиғалар санын шектеу үшін KLSRV_EVP_FIM_LIMIT кілтін жасаңыз. Келесі параметрлерді белгілеңіз:

  a. Кілт атауын KLSRV_EVP_FIM_LIMIT деп көрсетіңіз.

  b. Кілт түрін DWORD деп көрсетіңіз.

  c. Қабылданатын оқиғалар мәндерінің ауқымын 2000-нан 50 000-ға дейін белгілеңіз. Әдепкі бойынша, оқиғалар саны 20 000-ға тең.

- Оқиғаларды белгілі бір уақыт аралығына дейінгі дәлдікпен санау үшін KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC кілтін жасаңыз. Келесі параметрлерді белгілеңіз:

  a. Кілт атауын KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC деп көрсетіңіз.

  b. Кілт түрін DWORD деп көрсетіңіз.

  c. 120-600 секунд аралығындағы мәндер ауқымын көрсетіңіз. Әдепкі уақыт аралығы — 300 секунд.

- Көрсетілген уақыт мәнінен кейін бағдарлама уақыт аралығында өңделген оқиғалар санының белгіленген шектеуден аз болатынын тексеруі үшін KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC кілтін жасаңыз. Тексеру, оқиғаларды қабылдауға қойылған шектеуге жеткен кезде орындалады. Егер шарт орындалса, оқиғаларды дерекқорға сақтау қайта басталады. Келесі параметрлерді белгілеңіз:

  a. Кілт атауын KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC деп көрсетіңіз.

  b. Кілт түрін DWORD деп көрсетіңіз.

  c. 600-3 600 секунд аралығындағы мәндер ауқымын көрсетіңіз. Әдепкі уақыт аралығы — 1 800 секунд.

Егер кілттер жасалмаса, әдепкі бойынша мәндер қолданылады.

4. Басқару сервері қызметін қайта іске қосыңыз.

Файл тұтастығын басқару құрамдасынан оқиғаларды алуға қойылатын шектеулер конфигурацияланады. Файл тұтастығын басқару құрамдасы жұмысының нәтижесін **Осы құрылғыда Файл тұтастығын басқару / Жүйе толықтығын бақылау ережелері жиі іске қосылатын 10 ереже** және **Файл тұтастығын басқару / Жүйе толықтығын бақылау ережелері жиі іске қосылатын 10 құрылғы** есептерінде қарай аласыз.

Басқару серверіне техникалық қызмет көрсету

Басқару серверіне техникалық қызмет көрсету, Басқару сервері қалтасында орынды босатуға және қажет емес нысандарды жою арқылы дерекқордың өлшемін азайтуға мүмкіндік береді. Бұл қолданбаның өнімділігі мен сенімділігін жақсартуға көмектеседі. Басқару серверіне аптасына кемінде бір рет техникалық қызмет көрсету ұсынылады.

Басқару серверіне техникалық қызмет көрсету тиісті тапсырманың көмегімен орындалады. Басқару серверіне техникалық қызмет көрсету барысында бағдарлама келесі әрекеттерді орындайды:

- Сақтау қалтасынан қажет емес қалталар мен файлдарды жояды.
- Кестелерден қажет емес жазбаларды жояды («аспалы көрсеткіштер» деп те аталады).
- Кэшті тазартады.

- Дерекқорға қызмет көрсетеді (егер сіз SQL Server немесе PostgreSQL ДҚБЖ ретінде пайдалансаңыз):
  - дерекқорды қателер тұрғысынан тексереді (тек SQL Server үшін қолжетімді);
  - дерекқордың индекстерін қайта құрады;
  - дерекқордың статистикасын жаңартады;
  - дерекқорды қысады (қажет болса).

Басқару серверіне техникалық қызмет көрсету тапсырмасын жасау үшін:

1. Консоль ағашында, *Басқару серверіне техникалық қызмет көрсету* тапсырмасын жасау қажет болған Басқару сервері торабын таңдаңыз.
2. **Тапсырмалар** қалтасын таңдаңыз.
3. **Тапсырмалар** қалтасының жұмыс аймағындағы **Жаңа тапсырма** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
4. **Тапсырма түрін таңдау** шебері терезесінде **Басқару серверіне техникалық қызмет көрсету** тапсырма түрін таңдап, **Келесі** түймесін басыңыз.
5. Қызмет көрсету барысында Басқару серверінің дерекқорын қысу керек болса, онда **Параметрлер** шебері терезесінде **Дерекқорды сығу** жалаушасын қойыңыз.
6. Шебердің келесі қадамдарын орындаңыз.

Жасалған тапсырма **Тапсырмалар** қалтасының жұмыс аймағындағы тапсырмалар тізімінде көрсетіледі. Бір Басқару сервері үшін бір *Басқару серверіне техникалық қызмет көрсету* тапсырмасы ғана орындалуы мүмкін. Басқару сервері үшін *Басқару серверіне техникалық қызмет көрсету* тапсырмасы әлдеқашан жасалған болса, тағы бір *Басқару серверіне техникалық қызмет көрсету* тапсырмасын жасау мүмкін болмайды.

Жалпыға қолжетімді DNS серверлеріне қатынасу

Жүйелік DNS арқылы Kaspersky серверлеріне қатынасу мүмкін болмаса, Kaspersky Security Center жалпыға қолжетімді DNS серверлерін келесі ретпен пайдалана алады:

1. Google Public DNS (8.8.8.8);
2. Cloudflare DNS (1.1.1.1);
3. Alibaba Cloud DNS (223.6.6.6);
4. Quad9 DNS (9.9.9.9);
5. CleanBrowsing (185.228.168.168).

Бағдарлама DNS серверімен TCP/UDP қосылымын орнатқандықтан, DNS серверлеріне сұрауларда домен мекенжайлары мен Басқару серверінің жалпыға қолжетімді IP мекенжайы болуы мүмкін. Kaspersky Security Center жалпыға қолжетімді DNS серверін пайдаланса, деректерді өңдеу тиісті сервистік құпиялылық саясатымен реттеледі.

klscflag утилитасын пайдаланып жалпы DNS пайдалануды орнату үшін:

1. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Қоғамдық DNS пайдалануды өшіру үшін келесі пәрменді орындаңыз:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Қоғамдық DNS пайдалануды қосу үшін келесі пәрменді орындаңыз:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Пайдаланушыға хабарлау әдісі терезесі

Пайдаланушыға хабарлау әдісі терезесінде пайдаланушыға сертификатты ұялы құрылғыға орнату туралы хабарлау параметрлерін конфигурациялауға болады:

- **QR кодын шеберден көрсету**. Осы нұсқаны таңдаған кезде, орнату пакетіне сілтеме, құрылғыны қосу шебері жұмысының соңғы қадамында көрсетіледі.

- **QR кодын пайдаланушыға жіберу**. Осы нұсқаны таңдаған кезде, сіз пайдаланушыға құрылғыны қосу туралы хабарлау параметрлерін конфигурациялай аласыз.

Электрондық пошта арқылы параметрлері блогында пайдаланушыға сертификатты өз ұялы құрылғысына орнату туралы электрондық пошта хабарлары көмегімен хабарлау параметрлерін конфигурациялай аласыз. Осылай хабарлау әдісі, SMTP сервері конфигурацияланған болса ғана қолжетімді.

SMS арқылы параметрлері блогында пайдаланушыға сертификатты өз ұялы құрылғысына орнату туралы SMS хабарлары көмегімен хабарлау параметрлерін конфигурациялай аласыз. Осылай хабарлау әдісі, SMS хабарландырулары конфигурацияланған болса ғана қолжетімді.

Электрондық пошта арқылы және **SMS арқылы** параметрлері блогында **Хабарды өңдеу** сілтемесі бойынша хабарландыру мәтінін қарап шығып, қажет болса түзетіңіз.

Құрылғы таңдаулары терезесі

Құрылғыны таңдау тізімінен таңдауды таңдаңыз. Тізімде алдын ала анықталған таңдаулар мен пайдаланушы жасаған таңдаулар бар.

Сіз **Құрылғы таңдаулары** бөлімінің жұмыс аймағындағы құрылғыларды таңдау туралы толық ақпаратты көре аласыз.

Жасалатын нысанның атауын анықтау терезесі

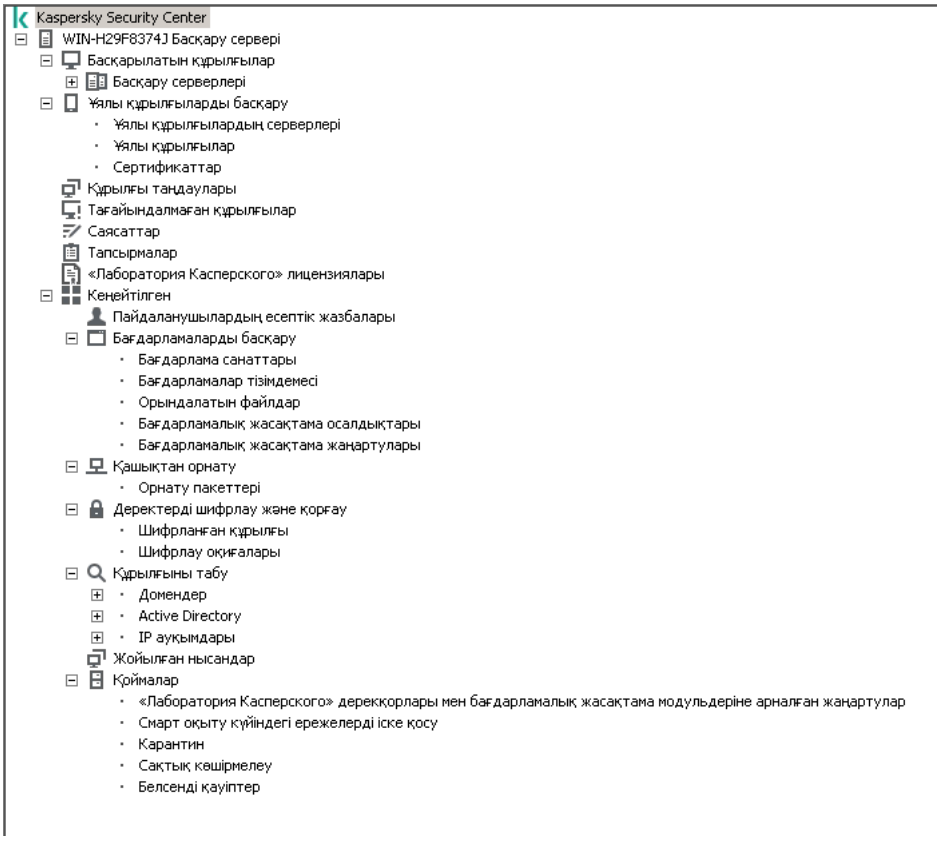
Терезеде жасалатын нысанның атауын көрсетіңіз. Атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

Басқару интерфейсімен жұмыс істеу ерекшеліктері

Бұл бөлімде Kaspersky Security Center басты терезесіндегі жұмыс тәсілдерінің сипаттамасы берілген.

Консоль ағашы

Консоль ағашы (төмендегі суретті қараңыз) желіде қалыптасқан Басқару серверлері иерархиясын, олардың басқару топтарының құрылымын, сондай-ақ бағдарламаның басқа нысандарын (мысалы, **Қоймалар** және **Бағдарламаларды басқару** қалталары) көрсетуге арналған. Kaspersky Security Center атаулар кеңістігінде, орнатылған және желі құрылымына қосылған Басқару серверлеріне сәйкес келетін сервер атаулары бар бірнеше түйіндер болуы мүмкін.



Консоль ағашы

Басқару сервері түйіні

Басқару сервері – <Құрылғы атауы> түйіні контейнер болып табылады және көрсетілген Басқару серверінің құрылымдық ұйымын көрсетеді.

Басқару сервері түйінінің жұмыс аймағында бағдарлама мен Басқару сервері басқаратын құрылғылардың ағымдағы күйі туралы жиынтық ақпарат бар. Жұмыс саласындағы ақпарат қойыншалар бойынша бөлінеді:

- **Мониторинг**. Нақты уақыттағы Мониторинг қойыншасы бағдарламаның жұмысы және клиент құрылғыларының ағымдағы күйі туралы ақпаратты көрсетеді. Әкімші үшін маңызды хабарлар (мысалы, осалдықтар, қателер, вирустарды анықтау туралы хабарлар) түспен ерекшеленеді. **Мониторинг** қойыншасындағы сілтемелер бойынша әкімшінің типтік тапсырмаларын орындауға болады (мысалы, клиент құрылғыларында қауіпсіздік бағдарламасын орнату және конфигурациялау), сонымен қатар консоль ағашының басқа қалталарына өтуге болады.

- **Статистика**. Онда тақырыптар бойынша топтастырылған диаграммалар жиынтығы бар (қорғаныс күйі, антивирустық статистика, жаңартулар және т.б.). Диаграммаларда визуалды түрде бағдарламаның жұмысы және клиент құрылғыларының күйі туралы ағымдағы ақпарат көрсетіледі.

- **Есептер**. Бағдарлама қалыптастыратын есеп үлгілерін қамтиды. Қойыншада сіз алдын ала орнатылған үлгілерден есептер құрастыра аласыз, сонымен қатар жеке есеп шаблондарын жасай аласыз.

- **Оқиғалар**. Бағдарлама жұмыс істеп тұрған кезде тіркелген оқиғалар туралы жазбаларды қамтиды. Оқуға және сұрыптауға ыңғайлы болу үшін жазбалар тақырыптық таңдауларға бөлінеді. Қойыншада сіз автоматты түрде жасалған оқиғалар үлгілерін көре аласыз, сонымен қатар өзіндік үлгілерді жасай аласыз.

Басқару сервері түйінінің құрамындағы қалталар

Басқару сервері – <Құрылғы атауы> түйінің құрамына келесі қалталар кіреді:

- **Басқарылатын құрылғылар**. Қалта басқару топтарының, топтық саясаттардың және топтық тапсырмалардың құрылымын сақтауға, көрсетуге, конфигурациялауға және өзгертуге арналған.

- **Ұялы құрылғыларды басқару**. Қалта ұялы құрылғыларды басқаруға арналған. **Ұялы құрылғыларды басқару** қалтасы келесі салынған қалталарды қамтиды:

  - **Ұялы құрылғылар серверлері**. iOS MDM серверлерін басқаруға арналған.

  - **Ұялы құрылғылар**. KES және iOS MDM мобильдік құрылғыларын басқаруға арналған.

  - **Сертификаттар**. Ұялы құрылғы сертификаттарын басқаруға арналған.

- **Құрылғыны таңдаулары**. Қалта барлық басқарылатын құрылғылар арасында белгілі бір критерийлерге сәйкес келетін құрылғыларды (құрылғыларды таңдау) жылдам таңдауға арналған. Мысалы, қауіпсіздік бағдарламасы орнатылмаған құрылғыларды жылдам таңдап, сол құрылғыларға өтуге болады (олардың тізімін қарау). Таңдалған құрылғылармен әрекеттерді орындауға, мысалы, оларға тапсырмалар беруге болады. Алдын ала орнатылған үлгілерді пайдалануға, сондай-ақ өзіндік (пайдаланушы) таңдаларын жасауға болады.

- **Тағайындалмаған құрылғылар**. Қалтада ешбір басқару тобына кірмейтін құрылғылардың тізімі бар. Сіз тағайындалмаған құрылғылармен әрекеттерді орындай аласыз, мысалы, оларды басқару топтарына көшіре аласыз немесе оларға қолданбалар орната аласыз.

- **Саясаттар**. Қалта саясаттарды қарауға және жасауға арналған.

- **Тапсырмалар**. Қалта тапсырмаларды қарауға және жасауға арналған.

- **Kaspersky лицензиясы**. Kaspersky бағдарламалары үшін қолжетімді лицензиялық кілттердің тізімін қамтиды. Қалтаның жұмыс аймағында сіз лицензиялық кілттер қоймасына жаңа лицензиялық кілттерді қоса аласыз, лицензиялық кілттерді басқарылатын құрылғыларға тарата аласыз, лицензиялық кілттерді пайдалану туралы есепті көре аласыз.

- **Қосымша**. Қалтада бағдарламаның әртүрлі функционалдық топтарына сәйкес келетін ішкі қалталар жиынтығы бар.

Қосымша қалтасы. Консоль ағашындағы қалталарды жылжыту

Қосымша қалтасының құрамына келесі қалталар кіреді:

- **Пайдаланушы есептік жазбалары**. Қалтада пайдаланушы есептік жазбалары тізімдері бар.

- **Бағдарламаларды басқару**. Қалта желідегі құрылғыларда орнатылған бағдарламаларды басқаруға арналған. **Бағдарламаларды басқару** қалтасы келесі салынған қалталарды қамтиды:

  - **Бағдарлама санаттары**. Бағдарламалардың пайдаланушы санаттарымен жұмыс істеуге арналған.

  - **Бағдарламалар тізімдемесі**. Желілік агенті орнатылған құрылғылардағы бағдарламалардың тізімін қамтиды.

  - **Орындалатын файлдар**. Желілік агенті орнатылған клиент құрылғыларында сақталған орындалатын файлдардың тізімін қамтиды.

  - **Бағдарламалық жасақтама осалдықтары**. Желілік агенті орнатылған құрылғылардағы бағдарламалық жасақтама осалдықтары тізімін қамтиды.

  - **Бағдарламалық жасақтама жаңартулары**. Құрылғыларға таратылуы мүмкін Басқару сервері алған бағдарламалардың жаңартуларының тізімін қамтиды.

  - **Өзге лицензияларды ескеру**. Лицензиялы бағдарламалар тобы тізімін қамтиды. Үшінші тараптың бағдарламалық жасақтамасына арналған лицензиялардың қолданысын және лицензия шегінің ықтимал бұзушылықтарын бақылау үшін лицензияланған қолданбалар топтарын пайдалануға болады.

- **Қашықтан орнату**. Қалта операциялық жүйелер мен бағдарламаларды қашықтан орнатуды басқаруға арналған. **Қашықтан орнату** қалтасы келесі салынған қалталарды қамтиды:

  - **Құрылғы кескіндерін орналастыру**. Құрылғыларда операциялық жүйелердің кескіндерін орналастыруға арналған.

  - **Орнату пакеттері**. Бағдарламаларды құрылғыларға қашықтан орнату үшін пайдалануға болатын орнату пакеттерінің тізімі бар.

- **Деректерді шифрлау және қорғау**. Қалта қатты және алынбалы дискілердегі деректерді шифрлау процесін басқаруға арналған.

- **Желіде сауалнама өткізу**. Қалта Басқару сервері орнатылған желіні көрсетуге арналған. Басқару сервері, желі құрылымы және оның құрамына кіретін құрылғылар туралы ақпаратты ұйым желісінде құрылған Windows желісінің, IP ауқымдарының және Active Directory сауалнамаларын тұрақты өткізіп тұру кезінде алады. Сауалнама нәтижелері тиісті қалталардың жұмыс аймақтарында көрсетіледі: **Домендер**, **IP ауқымдары** және **Active Directory**.

- **Қоймалар**. Қалта құрылғылардың күйін бақылау және оларға қызмет көрсету үшін пайдаланылатын нысандармен жұмыс істеуге арналған. **Қоймалар** қалтасы келесі салынған қалталарды қамтиды:

  - **Смарт оқыту күйінде ережелердің іске қосылуы**. Клиент құрылғыларында Смарт оқыту режимінде жұмыс істейтін Kaspersky Endpoint Security ережелері орындайтын анықтаулар тізімін қамтиды.

  - **Kaspersky БҚ жаңартулары мен патчтары**. Құрылғыларға таратылуы мүмкін Басқару сервері алған жаңартулардың тізімін қамтиды.

  - **Жабдық**. Ұйымның желісіне қосылған жабдықтардың тізімін қамтиды.

  - **Карантин**. Антивирустық бағдарламалар құрылғылардағы карантиндік қалталарға орналастырылған нысандардың тізімін қамтиды.

  - **Сақтық көшірмелеу**. Қалта құрылғылардағы зарарсыздандыру процесінде жойылған немесе өзгертілген файлдардың сақтық көшірмелерінің тізімін қамтиды.

  - **Кейін өңделетін файлдар**. Антивирустық бағдарламалар кешіктірілген зарарсыздандыру қажеттілігін анықтаған файлдардың тізімін қамтиды.

Сіз **Қосымша** қалтасына салынған қалталар жиынтығын өзгерте аласыз. Белсенді қолданылатын ішкі қалталарды **Қосымша** қалтасынан жоғары деңгейге жылжытуға болады. Жұмыста сирек қолданылатын қалталарды **Қосымша** қалтасына салуға болады.

*Салынған қалтаны **Қосымша** қалтасынан жылжыту үшін:*

1. Консоль ағашында **Қосымша** қалтасынан жылжытқыңыз келетін салынған қалтаны таңдаңыз.

2. Салынған қалтаның контекстік мәзірінде **Көру** → **Қосымша қалтасынан жылжыту** тармағын таңдаңыз.

> Сондай-ақ, **Қосымша** қалтасының жұмыс аймағында салынған қалтаны, салынған қалтаның атауы бар блоктағы **Қосымша қалтасынан жылжыту** сілтемесі бойынша **Қосымша** қалтасынан шығаруға болады.

*Қалтаны **Қосымша** қалтасына жылжыту үшін:*

1. Консоль ағашында **Қосымша** қалтасына жылжыту керек қалтаны таңдаңыз.

2. Қалтаның контекстік мәзірінде **Көру** → **Қосымша қалтасына жылжыту** тармағын таңдаңыз.

Жұмыс аймағындағы деректерді қалай жаңартуға болады

> Kaspersky Security Center бағдарламасында жұмыс аймағының деректері (құрылғылардың күйі, статистика және есептер сияқты) ешқашан автоматты түрде жаңартылмайды.

Жұмыс аймағындағы деректерді жаңарту үшін келесі әрекеттердің бірін орындаңыз:

- **F5** пернесін басыңыз;

- Консоль ағашындағы нысанның контекстік мәзірінде **Жаңарту** тармағын таңдаңыз;

- Жұмыс аймағыдағы () жаңарту белгішесін басыңыз.

Консоль шежіресі бойынша қалай жылжуға болады

Консоль шежіресі бойынша жылжу үшін құралдар тақтасындағы келесі түймелерді қолдануыңызға болады:

- – бір қадам артқа өту;
- – бір қадам алға өту;
- – бір деңгей жоғары өту.

Жұмыс аймағының жоғарғы оң жақ бұрышындағы навигация тізбегін пайдалануға да болады. Навигация тізбегі, сіз ағымдағы сәтте орналасқан консоль шежіресінің қалтасына апаратын толық жолды қамтиды. Соңғысын қоспағанда, тізбектің барлық элементтері консоль шежіресінің нысандарына келтірілген сілтемелер болып саналады.

Жұмыс аймағындағы нысанның сипаттары терезесін қалай ашуға болады

Басқару консолі нысандарының көп бөлігінің сипаттарын нысанның сипаттары терезесінде өзгертуге болады.

Жұмыс аймағындағы нысанның сипаттары терезесін ашу үшін келесі әрекеттердің бірін орындаңыз:

- нысанның контекстік мәзірінде **Сипаттар** тармағын таңдаңыз;
- нысанды таңдап, **ALT**+**ENTER** пернелерінің тіркесімін басыңыз.

Жұмыс аймағындағы нысандар тобын қалай таңдауға болады

Сіз жұмыс аймағындағы нысандар тобын таңдай аласыз. Нысандар тобын таңдауды, мысалы, арнайы құрылғыларды жасау, содан кейін оған арналған тапсырмаларды құрастыру үшін қолдануға болады.

Нысандар ауқымын таңдау үшін:

1. Бірінші ауқым нысанын таңдап, **SHIFT** пернесін басыңыз.
2. **SHIFT** пернесін басып тұрып, соңғы ауқым нысанын таңдаңыз.

   Ауқым таңдалады.

Бөлек нысандарды топқа біріктіру үшін:

1. Топтың құрамындағы бірінші нысанды таңдап, **CTRL** пернесін басыңыз.
2. **CTRL** пернесін басып тұрып, топтың бөлек нысандарын таңдаңыз.

   Нысандар топқа біріктіріледі.

Жұмыс аймағындағы бағандар жиынтығын қалай өзгертуге болады

Басқару консолі жұмыс аймағында көрсетілетін бағандар жиынтығын өзгертуге мүмкіндік береді.

Жұмыс аймағындағы бағандар жиынтығын өзгерту үшін:

1. Бағандар жиынтығын өзгерткіңіз келетін консоль шежіресі нысанын таңдаңыз.
2. Қалтаның жұмыс аймағында **Бағандарды қосу/жою** сілтемесі бойынша бағандар жиынтығын конфигурациялау терезесін ашыңыз.
3. **Бағандарды қосу/жою** терезесінде көрсету үшін бағандар жиынтығын құрастырыңыз.

Анықтамалық ақпарат

Бұл бөлімдегі кестелерде Басқару консолі нысандарының контекстік мәзірі, сондай-ақ консоль ағашы нысандары мен жұмыс аймағының күйлері туралы қысқаша ақпарат берілген.

Контекстік мәзір пәрмендері

Бұл бөлімде басқару консолі нысандары және сәйкес контекстік мәзір элементтері (төмендегі кестені қараңыз) тізімі берілген.

Басқару консолі нысандарының контекстік мәзірінің элементтері

Нысан	Мәзір тармағы	Мәзір тармағының мақсаты
Контекстік мәзірдің жалпы тармақтары	**Іздеу**	Құрылғыларды іздеу терезесін ашу.
	Жаңарту	Таңдалған нысанның көрсетілуін жаңарту.
	Тізімді экспорттау	Ағымдағы тізімді файлға экспорттау.
	Сипаттар	Таңдалған нысанның сипаттары терезесін ашу.
	Көру → Бағандарды қосу/жою	Жұмыс аймағындағы нысандар кестесінде бағандарды қосу немесе жою.
	Көру → Ірі белгішелер	Жұмыс аймағындағы нысандарды ірі белгішелер түрінде көрсету.
	Көру → Шағын белгішелер	Жұмыс аймағындағы нысандарды шағын белгішелер түрінде көрсету.
	Көру → Список	Жұмыс аймағындағы нысандарды тізім түрінде көрсету.
	Көру → Кесте	Жұмыс аймағындағы нысандарды кесте түрінде көрсету.
	Көру→ Интерфейсті конфигурациялау	Басқару консолі элементтерін көрсетуді конфигурациялау.
Kaspersky Security Center	**Жасау → Басқару сервері**	Консоль шежіресіне Басқару серверін қосу.
<Басқару сервері атауы>	**Басқару серверіне қосылу**	Басқару серверіне қосу.
	Басқару серверінен ажырату	Басқару серверінен ажырату.

Нысан	Мәзір тармағы	Мәзір тармағының мақсаты
Басқарылатын құрылғылар	**Бағдарламаны орнату**	Бағдарламаны қашықтан орнату шеберін іске қосу.
	Түрі → Интерфейсті конфигурациялау	Интерфейс элементтерін көрсетуді конфигурациялау.
	Жою	Басқару серверін консоль шежіресінен жою.
	Бағдарламаны орнату	Басқару тобы үшін қашықтан орнату шеберін іске қосу.
	Вирустар есептегішін нөлдеу	Басқару тобы құрамына кіретін құрылғылар үшін вирустар есептегішін нөлдеу.
	Қауіп-қатер туралы есепті көру	Басқару топтарының құрамына кіретін құрылғылардың вирустық белсенділігі мен қауіп-қатері туралы есепті жасау.
	Жасау → Топ	Басқару тобын жасау.
	Барлық тапсырма → Жаңа топ құрылымы	Домендер құрылымы немесе Active Directory негізінде басқару топтары құрылымын жасау.
	Барлық тапсырма → Хабарды көрсету	Басқару тобына кіретін құрылғылардың пайдаланушылары хабарын жасау шеберін іске қосу.
Басқарылатын құрылғылар → Басқару серверлері	**Жасау → Қосалқы Басқару сервері**	Қосалқы Басқару серверін қосу шеберін іске қосу.
	Жасау → Виртуалды Басқару сервері	Виртуалды Басқару серверін жасау шеберін іске қосу.
Мобильді құрылғыларды басқару → Ұялы құрылғылар	**Жасау → Ұялы құрылғы**	Пайдаланушының жаңа ұялы құрылғысын қосу.
Мобильді құрылғыларды басқару → Сертификаттар	**Жасау → Сертификат**	Сертификат жасау.
	Жасау → Ұялы құрылғы	Пайдаланушының жаңа ұялы құрылғысын қосу.
Құрылғы таңдаулары	**Жасау → Жаңа таңдау**	Құрылғы таңдауларын жасау.
	Барлық тапсырма → Импорттау	Таңдауды файлдан импорттау.
Kaspersky лицензиялары	**Белсендіру кодын немесе кілт файлын қосу**	Лицензиялық кілтті Басқару сервері қоймасына қосу.
	Бағдарламаны белсендіру	Бағдарламаны белсендіру тапсырмасын жасау шеберін іске қосу.
	Лицензиялық кілттерді пайдалану туралы есеп	Клиент құрылғыларында лицензиялық кілттер туралы есепті жасау және қарап шығу.
Бағдарламаларды басқару → Бағдарлама санаттары	**Жасау → Санат**	Бағдарлама санатын жасау.
Бағдарламаларды басқару → Бағдарламалар тізімдемесі	**Сүзгі**	Бағдарламалар тізімі үшін сүзгіні конфигурациялау.
	Бақыланатын бағдарламалар	Бағдарламаларды орнату туралы оқиғалар жарияланымын конфигурациялау.
	Орнатылмаған бағдарламаларды жою	Желінің құрылғыларында қазір орнатылмаған бағдарламалар туралы ақпаратты тізімінен жою.
Бағдарламаларды басқару → Бағдарламалық жасақтама жаңартулары	**Жаңартулардың Лицензиялық келісімдерін қабылдау**	Бағдарламалық жасақтама жаңартуының Лицензиялық келісімдерін қабылдау.
Бағдарламаларды басқару → Үшінші тарап лицензияларын пайдалану	**Жасау → Лицензиялы бағдарламалар тобы**	Лицензиялы бағдарламалар тобын жасау.

Нысан	Мәзір тармағы	Мәзір тармағының мақсаты
Қашықтан орнату → Орнату пакеттері	**Ағымдағы бағдарлама нұсқаларын көрсету**	Интернет-серверлерде орналастырылған Kaspersky бағдарламаларының ағымдағы нұсқаларының тізімін көру.
	Жасау → Орнату пакеті	Орнату пакетін жасау.
	Барлық тапсырма → Дерекқорларды жаңарту	Орнату пакеттеріндегі бағдарламалардың дерекқорларын жаңарту.
	Барлық тапсырма → Автономды пакеттердің жалпы тізімін көрсету	Орнату пакеттері үшін жасалған автономды орнату пакеттері тізімін көру.
Құрылғыны табу → Домендер	**Барлық тапсырма → Құрылғы белсенділігі**	Басқару серверінің желідегі құрылғылар белсенділігінің болмауына жауап қайтаруы параметрлерін конфигурациялау.
Құрылғыны табу → IP ауқымдары	**Жасау → IP ауқымы**	IP ауқымын жасау.
Қоймалар → Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар	**Жаңартуларды жүктеп алу**	Жаңартуларды Басқару серверінің қоймасына жүктеу тапсырмасы сипаттары терезесін ашу.
	Жаңартуларды жүктеп алу параметрлері	Жаңартуларды Басқару серверінің қоймасына жүктеу тапсырмасының параметрлерін конфигурациялау.
	Антивирустық дерекқорларды пайдалану туралы есеп	Дерекқорлардың нұсқалары туралы есепті жасау және қарап шығу.
	Барлық тапсырма → Жаңартулар қоймасын тазалау	Басқару серверіндегі жаңартулар қоймасын тазалау.
Қоймалар → Жабдық	**Жасау → Құрылғы**	Желілік құрылғы жасау.

Басқарылатын құрылғылар тізімі Бағандар мәні

Төмендегі кестеде басқарылатын құрылғылар тізімінің бағандарының атаулары мен сипаттамалары келтірілген.

Басқарылатын құрылғылар тізімінің бағандарының мәні

Бағанның атауы	Мән
Атауы	Клиент құрылғысының NetBIOS атауы. Құрылғы атауының белгішелерінің сипаттамасы қолданбада берілген.
Операциялық жүйенің түрі	Клиент құрылғысының операциялық жүйесінің түрі.
Windows домені	Клиент құрылғысы орналасқан Windows домені атауы.
Желілік агент орнатылған	Желілік агенттің клиент құрылғысына орнату нәтижесі: *Иә*, *Жоқ*, *Белгісіз*.
Желілік агент іске қосулы	Желілік агенттің жұмыс істеу нәтижесі: *Иә*, *Жоқ*, *Белгісіз*.
Нақты уақыт режимінде қорғау	Қауіпсіздік бағдарламасы орнатылған: *Иә*, *Жоқ*, *Белгісіз*.
Басқару серверіне соңғы қосылу уақыты	Клиент құрылғысы Басқару серверіне қосылған сәттен бастап өткен уақыт.
Антивирустық дерекқорларды соңғы рет жаңарту уақыты	Басқарылатын құрылғылар соңғы жаңартылғаннан бері өткен уақыт.
Күйі	Клиент құрылғысының ағымдағы күйі (*ОК, критикалық, ескерту).*

Бағанның атауы	Мән
Күйдің сипаттамасы	Клиент құрылғысы күйінің *Критикалық* немесе *Ескерту* болып өзгеруінің шарттары. Құрылғының күйі келесі шарттармен *Ескерту* немесе *Критикалық* болып өзгереді: • Қауіпсіздік бағдарламасы орнатылмаған. • Тым көп вирус анықталды. • Нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше. • Зиянды бағдарлама сканерлеуі ұзақ уақыт орындалмады. • Дерекқорлар ескірген. • Қосылмағанына көп болды. • Белсенді қауіптер анықталды. • Қайта іске қосу керек. Құрылғыны қайта іске қосу себебі келесінің бірі болуы мүмкін: • Анықталмаған қайта іске қосу себебі. • Бағдарлама қайта іске қосуға дейін жұмыс істемейді. • Жаңартуды аяқтау үшін қайта іске қосу қажет; бағдарлама жұмыс істеуде. • Жаңартуды қолдану үшін қайта іске қосу қажет. • Сканерлеуді немесе емдеуді аяқтау үшін қайта жүктеу керек. • Қашықтан орнатуды/жоюды аяқтау үшін қайта іске қосу қажет. • Дискідегі деректерді шифрлауды аяқтау. Құрылғы күйлерін ауыстыруды конфигурациялаған кезде, себептерді орнатуға болады. • Үйлесімді емес бағдарламалар орнатылды. • Бағдарламалық жасақтама осалдықтары анықталды. • Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады. • Жарамсыз шифрлау күйі. • Ұялы құрылғы параметрлері саясатқа жауап бермейді. • Өңделмеген қауіпсіздік мәселелері табылды. • Бағдарлама анықтаған құрылғы күйі. • Құрылғыда бос орын жоқ. • Лицензияның қолданылу мерзімі жақында аяқталады. Құрылғының күйі келесі себептермен тек *Критикалық* болып өзгереді: • Лицензия мерзімі өтті. • Құрылғы басқарылмайтын күйге айналды. • Қорғаныс өшірілген. • Қауіпсіздік бағдарламасы іске қосылмаған. Клиент құрылғыларындағы Kaspersky басқарылатын бағдарламалары күй сипаттамаларының тізімін толықтыра алады. Kaspersky Security Center осы құрылғыдағы Kaspersky басқарылатын бағдарламаларынан клиент құрылғысы күйінің сипаттамасын ала алады. Егер құрылғыға басқарылатын бағдарламалар тағайындаған күй Kaspersky Security Center тағайындаған күйге сәйкес келмесе, Басқару консолінде құрылғының қауіпсіздігі үшін ең критикалық күй көрсетіледі. Мысалы, егер басқарылатын бағдарламалардың бірі құрылғыға *Критикалық* күйін тағайындап, Kaspersky Security Center бағдарламасы *Ескерту* күйін тағайындаған болса, онда Басқару консолінде құрылғы үшін *Критикалық* күйі және басқарылатын бағдарламадан осы күйдің сипаттамасы көрсетіледі.
Ақпарат жаңартылды	Клиент құрылғысы Басқару серверімен соңғы сәтті синхрондалғаннан бері өткен уақыт (яғни, желінің соңғы сауалнамасынан бастап).
DNS атауы	Клиент құрылғысының DNS домен атауы.
DNS домені	Негізгі DNS суффиксі.
IP мекенжайы	Клиент құрылғысы IP мекенжайы. IPv4 мекенжайын қолдану ұсынылады.
Байланысқа соңғы рет шығу уақыты	Клиент құрылғысының желіде көрінуі ұзақтығы.
Соңғы рет толық сканерлеу уақыты	Пайдаланушының талабы бойынша қауіпсіздік бағдарламасы тарапынан клиент құрылғысын соңғы тексеру күні мен уақыты.
Анықталған қауіптердің жалпы саны	Табылған қауіп-қатерлер саны.
Нақты уақыт режимінде қорғау күйі	Нақты уақыт режимінде қорғау күйі: *Іске қосылды, Орындалуда, Орындалуда (ең жоғары қорғау), Орындалуда (ең жоғары жылдамдық), Орындалуда (ұсынылатын параметрлер), Орындалуда (реттелетін параметрлер), Тоқтатылды, Кідіртілді, Сәтсіз аяқталды.*
Байланыстың IP мекенжайы	Kaspersky Security Center Басқару серверіне қосылуға арналған IP мекенжайы.
Желілік агенттің нұсқасы	Желілік агенттің нұсқасы.
Бағдарламаның нұсқасы	Клиент құрылғысында орнатылған қауіпсіздік бағдарламасының нұсқасы.

Бағанның атауы	Мән
Антивирустық дерекқорды шығару уақыты	Антивирустық дерекқорлардың нұсқасы.
Жүйенің соңғы іске қосылған уақыты	Клиент құрылғысын соңғы рет қосу күні мен уақыты.
Қайта іске қосу керек	Клиент құрылғысын қайта іске қосу керек.
Тарату нүктесі	Осы клиент құрылғысы үшін тарату нүктесінің рөлін атқаратын құрылғы атауы.
Сипаттама	Желіні сканерлеу кезінде алынған клиент құрылғысының сипаттамасы.
Шифрлау күйі	Клиент құрылғысының деректерін шифрлау күйі.
WUA күйі	Клиент құрылғысының Windows жаңарту агентінің күйі. *Иә* мәні Windows Update арқылы Басқару серверінен жаңартуларды алатын клиент құрылғыларына сәйкес келеді. *Жоқ* мәні Windows Update арқылы басқа көздерден жаңартуларды алатын клиент құрылғыларына сәйкес келеді.
Операциялық жүйенің биттік өлшемі	Клиент құрылғысының операциялық жүйесінің бит өлшемі.
Спамнан қорғаудың күйі	Спамнан қорғау құрамдасының күйі: *Орындалуда, Іске қосылды, Тоқтатылды, Кідіртілді, Сәтсіз аяқталды, Белгісіз.*
Деректердің жайылып кетуіне жол бермеу күйі	Деректердің жайылып кетуінен қорғау құрамдасының күйі: *Орындалуда, Іске қосылды, Тоқтатылды, Кідіртілді, Сәтсіз аяқталды, Белгісіз.*
Бірлескен жұмыс серверлерінің қорғаныс күйі	Мазмұнды сүзу құрамдасының күйі: *Орындалуда, Іске қосылды, Тоқтатылды, Кідіртілді, Сәтсіз аяқталды, Белгісіз.*
Пошталық серверлердің антивирустық қорғаныс күйі	Пошталық серверлердің антивирустық қорғаныс құрамдасының күй: *Орындалуда, Іске қосылды, Тоқтатылды, Кідіртілді, Сәтсіз аяқталды, Белгісіз.*
Endpoint Sensor күйі	Endpoint Detection and Response component (KATA) құрамдасының күйі: *Орындалуда, Іске қосылды, Тоқтатылды, Кідіртілді, Сәтсіз аяқталды, Белгісіз.*
Жасалған күні	<Құрылғы атауы> белгішесі жасалған уақыт. Бұл атрибут әртүрлі оқиғаларды бір-бірімен салыстыру үшін қолданылады.
Виртуалды немесе қосалқы Басқару серверінің атауы	Виртуалды немесе қосалқы Басқару серверінің атауы. Бұл баған әртүрлі Басқару серверлеріндегі құрылғыларды қамтитын тізімдерде ғана қолжетімді.
Тектік топ	<Құрылғы атауы> белгішесі орналасқан басқару тобының атауы. Бұл баған әртүрлі Басқару серверлеріндегі құрылғыларды қамтитын тізімдерде ғана қолжетімді.
Басқа Басқару серверімен басқарылады	Параметр келесі мәндердің біріне ие болуы мүмкін: • True – егер қауіпсіздік бағдарламаларын құрылғыға қашықтан орнатқан кезде құрылғыны басқа Басқару сервері басқаратыны анықталса. • False – олай болмаса.
Операциялық жүйе құрастырылымы	Операциялық жүйенің құрастыру нөмірі. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық жинақ нөмірлерін іздеуді конфигурациялауға болады.
Операциялық жүйе шығарылымының идентификаторы	Операциялық жүйе шығарылымының идентификаторы. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш шығарылым идентификаторы болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық шығарылым идентификаторы нөмірлерін іздеуді конфигурациялауға болады.

Құрылғылар, тапсырмалар және саясат күйлері

Төмендегі кестеде консоль ағашында және Басқару консолінің жұмыс аймағында құрылғы атауларының, тапсырмалар мен саясаттардың жанында пайда болатын белгішелер тізімі берілген. Бұл белгішелер нысандардың күйін сипаттайды.

Құрылғылар, тапсырмалар және саясат күйлері

Белгіше	Күй
	Желіде табылған және қандай да бір басқару тобының құрамына кірмейтін жұмыс станцияларына арналған операциялық жүйесі бар құрылғы.
	*OK* күйі бар басқару тобының құрамына кіретін жұмыс станцияларына арналған операциялық жүйесі бар құрылғы
	*Ескерту* күйі бар басқару тобының құрамына кіретін жұмыс станцияларына арналған операциялық жүйесі бар құрылғы
	*Критикалық* күйі бар басқару тобының құрамына кіретін жұмыс станцияларына арналған операциялық жүйесі бар құрылғы
	Басқару серверімен қосылымы жоғалған басқару тобының құрамына кіретін жұмыс станцияларына арналған операциялық жүйесі бар құрылғы.
	Желіде табылған және қандай да бір басқару тобының құрамына кірмейтін серверлерге арналған операциялық жүйесі бар құрылғы.
	*OK* күйі бар басқару тобының құрамына кіретін серверлерге арналған операциялық жүйесі бар құрылғы
	*Ескерту* күйі бар басқару тобының құрамына кіретін серверлерге арналған операциялық жүйесі бар құрылғы
	*Критикалық* күйі бар басқару тобының құрамына кіретін серверлерге арналған операциялық жүйесі бар құрылғы
	Басқару серверімен қосылымы жоғалған басқару тобының құрамына кіретін серверлерге арналған операциялық жүйесі бар құрылғы.
	Желіде табылған және қандай да бір басқару тобының құрамына кірмейтін ұялы құрылғы.
	*OK* күйі бар басқару тобының құрамына кіретін ұялы құрылғы.
	*Ескерту* күйі бар басқару тобының құрамына кіретін ұялы құрылғы.
	*Критикалық* күйі бар басқару тобының құрамына кіретін ұялы құрылғы.
	Басқару серверімен қосылымы жоғалған басқару тобының құрамына кіретін ұялы құрылғы.
	Желіде табылған және қандай да бір басқару тобының құрамына кірмейтін UEFI деңгейіндегі қорғанысы бар құрылғы. UEFI деңгейлі қорғанысты құрылғы желіде.
	Желіде табылған және қандай да бір басқару тобының құрамына кірмейтін UEFI деңгейіндегі қорғанысы бар құрылғы. UEFI деңгейлі қорғанысты құрылғы желіде емес.
	Басқару тобының құрамына кіретін UEFI деңгейлі қорғанысты құрылғының күйі *OK*. UEFI деңгейлі қорғанысты құрылғы желіде.
	Басқару тобының құрамына кіретін UEFI деңгейлі қорғанысты құрылғының күйі *OK*. UEFI деңгейлі қорғанысты құрылғы желіде емес.
	Басқару тобының құрамына кіретін UEFI деңгейлі қорғанысты құрылғының күйі *Ескерту*. UEFI деңгейлі қорғанысты құрылғы желіде.
	Басқару тобының құрамына кіретін UEFI деңгейлі қорғанысты құрылғының күйі *Ескерту*. UEFI деңгейлі қорғанысты құрылғы желіде емес.
	Басқару тобының құрамына кіретін UEFI деңгейлі қорғанысты құрылғының күйі *Критикалық*. UEFI деңгейлі қорғанысты құрылғы желіде.
	Басқару тобының құрамына кіретін UEFI деңгейлі қорғанысты құрылғының күйі *Критикалық*. UEFI деңгейлі қорғанысты құрылғы желіде емес.
	Белсенді саясат.

	Белсенді емес саясат.
	Негізгі Басқару серверінде құрылған топтан иеленген белсенді саясат.
	Иерархияның жоғарғы деңгейдегі тобынан иеленген белсенді саясат.
	Тапсырма (топтық, Басқару серверінің немесе арнайы құрылғылар үшін) *Жоспарланған* немесе *Сәтті аяқталды* күйінде.
	Тапсырма (топтық, Басқару серверінің немесе арнайы құрылғылар үшін) *Орындалуда* күйінде.
	Тапсырма (топтық, Басқару серверінің немесе арнайы құрылғылар үшін) *Сәтсіз аяқталды* күйінде.
	Негізгі Басқару серверінде құрылған топтан иеленген тапсырма.
	Иерархияның жоғарғы деңгейдегі тобынан иеленген тапсырма.

Басқару консоліндегі файлдар күйінің белгішелері

Файлдармен жұмыс істеуді жеңілдету үшін Kaspersky Security Center Басқару консолінде файл атауларының жанында белгішелер көрсетіледі (төмендегі кестені қараңыз). Белгішелер, клиент құрылғыларындағы Kaspersky басқарылатын бағдарламалары тарапынан файлдарға тағайындалған күйлер туралы сигнал береді. Белгішелер **Карантин**, **Сақтық көшірмелеу** және **Белсенді қауіптер** қалталарының жұмыс аймағында көрсетіледі.

Күйлер, нысан орналасқан клиент құрылғысында орнатылған Kaspersky Endpoint Security бағдарламасы тарапынан нысандарға тағайындалады.

Белгішелердің файл күйлеріне сәйкестігі

Белгіше	Күй
	*Вирус жұққан* күйі бар файл.
	*Ескерту* немесе *Вирус жұққан болуы мүмкін* күйі бар файл.
	*Пайдаланушы қосқан* күйі бар файл.
	*Жалған позитив* күйі бар файл.
	*Емделді* күйі бар файл.
	*Жойылды* күйі бар файл.
	*Вирус жұқпаған, Құпиясөзбен қорғалған* немесе *Kaspersky компаниясына жіберілуі керек* күйі бар **Карантин** қалтасындағы файл. Белгішенің жанында күй сипаттамасы болмаса, демек, клиент құрылғысындағы Kaspersky басқарылатын бағдарламасы Kaspersky Security Center-ге белгісіз күйді тағайындаған.
	*Вирус жұқпаған, Құпиясөзбен қорғалған* немесе *Kaspersky компаниясына жіберілуі керек* күйі бар **Сақтық көшірмелеу** қалтасындағы файл. Белгішенің жанында күй сипаттамасы болмаса, демек, клиент құрылғысындағы Kaspersky басқарылатын бағдарламасы Kaspersky Security Center-ге белгісіз күйді тағайындаған.
	*Вирус жұқпаған, Құпиясөзбен қорғалған* немесе *Kaspersky компаниясына жіберілуі керек* күйі бар **Белсенді қауіптер** қалтасындағы файл. Белгішенің жанында күй сипаттамасы болмаса, демек, клиент құрылғысындағы Kaspersky басқарылатын бағдарламасы Kaspersky Security Center-ге белгісіз күйді тағайындаған.

Деректерді іздеу және экспорттау

Бұл бөлімде деректерді іздеу тәсілдері туралы және деректерді экспорттау туралы ақпарат қамтылған.

Құрылғыларды іздеу

Kaspersky Security Center белгіленген критерийлер негізінде құрылғыларды іздеуге мүмкіндік береді. Іздеу нәтижелерін мәтіндік файлға сақтауға болады.

Іздеу функциясы келесі құрылғыларды табуға мүмкіндік береді:

- Басқару сервері және оның қосалқы Серверлері топтарындағы клиент құрылғылары;
- Басқару сервері мен оның қосалқы Серверлері басқаратын тағайындалмаған құрылғылар.

Басқару тобына кіретін клиент құрылғыларын іздеу үшін:

1. Консоль ағашында басқару топтары қалтасын таңдаңыз.
2. Басқару тобы қалтасының контекстік мәзірінде **Іздеу** тармағын таңдаңыз.
3. **Іздеу** терезесінің қойыншаларында құрылғыларды іздеу критерийлерін көрсетіңіз және **Қазір табу** түймесін басыңыз.

   Нәтижесінде, белгіленген іздеу критерийлеріне сәйкес келетін құрылғылар **Іздеу** терезесінің төменгі жағындағы кестеде көрсетіледі.

Тағайындалмаған құрылғыларды іздеу үшін:

1. Консоль ағашында **Тағайындалмаған құрылғылар** қалтасын таңдаңыз.
2. **Тағайындалмаған құрылғылар** қалтасының контекстік мәзірінен **Іздеу** опциясын таңдаңыз.
3. **Іздеу** терезесінің қойыншаларында құрылғыларды іздеу критерийлерін көрсетіңіз және **Қазір табу** түймесін басыңыз.

   Нәтижесінде, белгіленген іздеу критерийлеріне сәйкес келетін құрылғылар **Іздеу** терезесінің төменгі жағындағы кестеде көрсетіледі.

Құрылғыларды басқару топтары құрамына кіріп-кірмейтініне қарамастан іздеу үшін:

1. Консоль ағашында **Басқару сервері** түйінін таңдаңыз.
2. Басқару сервері түйінінің контекстік мәзірінде **Іздеу** тармағын таңдаңыз.
3. **Іздеу** терезесінің қойыншаларында құрылғыларды іздеу критерийлерін көрсетіңіз және **Қазір табу** түймесін басыңыз.

   Нәтижесінде, белгіленген іздеу критерийлеріне сәйкес келетін құрылғылар **Іздеу** терезесінің төменгі жағындағы кестеде көрсетіледі.

Іздеу терезесінде терезенің жоғарғы оң жақ бұрышындағы ашылмалы тізім арқылы басқару топтары мен қосалқы Басқару серверлерін іздеуге болады. Басқару топтары мен қосалқы Басқару серверлерін іздеу **Тағайындалмаған құрылғылар** қалтасынан **Іздеу** терезесін ашу кезінде қолжетімсіз.

Құрылғыларды табу үшін **Іздеу** терезесінің өрістеріндегі тұрақты өрнектерді пайдалануға болады.

Іздеу терезесінде толық мәтіндік іздеу мүмкіндігі қолжетімді емес:

- **Сипаттама** өрісіндегі **Желі** қойыншасында;
- **Құрылғы**, **Өндіруші** және **Сипаттама** өрістеріндегі **Жабдық** қойыншасында.

Құрылғыны іздеу параметрлері

Төменде басқарылатын құрылғыларды іздеу параметрлерінің сипаттамасы келтірілген. Іздеу нәтижелері терезенің төменгі жағындағы кестеде көрсетіледі.

Желі

Желі қойыншасында құрылғыларды іздеу өлшемшарттарын олардың желілік деректері негізінде конфигурациялауға болады:

- **Құрылғының атауы немесе IP мекенжайы**

  Windows желісіндегі құрылғы атауы (NetBIOS атауы) немесе IPv4 мекенжайы не IPv6 мекенжайы.

- **Windows домені**

  Көрсетілген Windows доменіне кіретін барлық құрылғылар көрсетіледі.

- **Басқару тобы**

  Көрсетілген басқару тобына кіретін құрылғылар көрсетіледі.

- **Сипаттама**

  Құрылғы сипаттары терезесінде қамтылған мәтін: **Жалпы** бөлімінің **Сипаттама** өрісінде.

  Сипаттама мәтінінде келесі таңбаларды қолдануға болады:

  - Бір сөздің ішінде:

    - ***.** 0 немесе одан да көп таңбадан ұзын кез келген жолды алмастырады.

    Мысалы:

    Сервер, **Серверлік** сөздерін сипаттау үшін **Сервер*** жолын қолдануға болады.

    - **?.** Кез келген бір таңбаны ауыстырады.

    Мысалы:

    Құралдар немесе **Құралдан** сөздерін сипаттау үшін **Құралда?** жолын қолдануға болады.

    Жұлдызша (*****) немесе сұрақ белгісі (**?**) мәтін сипаттамасында бірінші таңба ретінде қолданылуы мүмкін емес.

  - Бірнеше сөздерді байланыстыру үшін:

    - Бос орын. Сипаттамаларында аталған сөздердің кез келгені бар барлық құрылғыларды көрсетеді.

Мысалы:

Қосалқы немесе **Виртуалдық** сөзін қамтитын сөйлемшені сипаттау үшін **Қосалқы Виртуалды** жолын қолдануға болады.

- **+**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болуын білдіреді.

Мысалы:

Қосалқы сөзін де, **Виртуалды** сөзін де қамтитын сөйлемшені сипаттау үшін **+Қосалқы+Виртуалды** жолын қолдануға болады.

- **-**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болмауын білдіреді.

Мысалы:

Қосалқы сөзі болуы, бірақ **Виртуалды** сөзі болмауы тиісті сөйлемшені сипаттау үшін **+Қосалқы-Виртуалды** жолын қолдануға болады.

- **"<мәтін үзіндісі>"**. Тырнақшаға алынған мәтін үзіндісі мәтінде толығымен болуы керек.

Мысалы:

Қосалқы Сервер сөзтіркесін қамтитын сөйлемшені сипаттау үшін, **"Қосалқы Сервер"** жолын қолдануға болады.

- **IP ауқымы**

  Бұл параметр қосулы болса, енгізу өрістерінде сіз іздеген құрылғылар кіруі тиісті аралықтың бастапқы және соңғы IP мекенжайларын көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Басқа Басқару серверімен басқарылады**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Таңдауға тек басқа Басқару серверлері басқаратын клиент құрылғылары қосылады.
  - **Жоқ**. Бір басқару серверімен басқарылатын клиент құрылғылары ғана есепке алынады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Тегтер

Тегтер қойыншасында бұған дейін басқарылатын құрылғылардың сипаттамаларына қосылған кілт сөздер (тегтер) бойынша құрылғыларды іздеуді конфигурациялауға болады:

- **Кем дегенде бір көрсетілген тег сәйкес келген жағдайда қолдану**

  Егер бұл параметр қосулы болса, іздеу нәтижелерінде сипаттамасында таңдалған тегтердің кемінде біреуі бар құрылғылар көрсетіледі.

  Егер бұл параметр өшірулі болса, іздеу нәтижелерінде тек сипаттамаларында барлық таңдалған тегтері бар құрылғылар көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Тег болуы керек**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі бар құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Тег болмауы керек**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі жоқ құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

Active Directory

Active Directory қойыншасында құрылғыларды Active Directory бөлімшесінде (OU) немесе тобында іздеу керек екенін көрсетуге болады. Сондай-ақ, аталған Active Directory бөлімшесінің барлық еншілес бөлімшелерінен құрылғыны таңдауға қосуға болады. Құрылғыларды таңдау үшін келесі параметрлерді көрсетіңіз:

- **Құрылғы Active Directory ұйымдық бөлімшесінде орналасқан**

  Бұл параметр қосулы болса, енгізу өрісінде көрсетілген Active Directory ұйым бірлігіндегі құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Еншілес ұйымдық бөлімшелерін қосу**

  Бұл параметр қосулы болса, доменнің көрсетілген ұйымдық бірлігінің еншілес бөлімшелеріне кіретін құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы Active Directory тобының мүшесі болып табылады**

  Егер бұл параметр қосулы болса, енгізу өрісінде көрсетілген Active Directory тобындағы құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

Желілік белсенділік

Желілік белсенділік қойыншасында құрылғыларды іздеу өлшемшарттарын олардың желілік белсенділігі негізінде көрсетуге болады:

- **Бұл құрылғы тарату нүктесі болып табылады**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға тарату нүктелері болып табылатын құрылғылар қосылады.
  - **Жоқ**. Тарату нүктелері ретінде әрекет ететін құрылғылар таңдауға кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверімен байланысты үзбеу**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Қосулы**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы қойылған құрылғыларды қамтиды.
  - **Өшірулі**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы алынған құрылғыларды қамтиды.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қосылым профилі ауыстырылды**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға қосылым профилін ауыстырып қосу нәтижесінде Басқару серверіне қосылған құрылғылар кіреді.
  - **Жоқ**. Таңдауға қосылым профилін ауыстыру нәтижесінде басқару серверіне қосылған құрылғылар кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверіне соңғы қосылу уақыты**

  Осы жалаушаны пайдаланып, Басқару серверіне соңғы қосылу уақыты бойынша құрылғыларды іздеу өлшемшартын белгілей аласыз.

  Егер жалауша қойылса, енгізу өрістерінде, клиент құрылғысында орнатылған Желілік агенттің Басқару серверіне соңғы қосылуы орындалған аралықтың мәндерін (күні мен уақыты) көрсетуге болады. Таңдауға белгіленген аралыққа сәйкес келетін құрылғылар қосылады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Жаңа құрылғылар желі сауалнамасымен анықталды**

  Соңғы бірнеше күнде желіде сауалнама өткізу кезінде табылған жаңа құрылғыларды іздеу.

  Егер бұл параметр қосулы болса, онда **Анықтау кезеңі (тәу)** өрісінде көрсетілген күндер санында құрылғыларды анықтау процесінде табылған жаңа құрылғылар ғана таңдауға қосылады.

  Егер бұл параметр өшірулі болса, онда құрылғыны анықтау процесінде табылған барлық құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы көрінеді**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Бағдарлама қазіргі уақытта желіде көрінетін құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қазіргі уақытта желіде көрінбейтін құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Бағдарлама

Бағдарлама қойыншасында құрылғыларды іздеу өлшемшарттарын таңдалған басқарылатын бағдарлама негізінде көрсетуге болады:

- **Бағдарлама атауы**

  Ашылмалы тізімде, Kaspersky бағдарламасының атауы бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады.

  Тізімде, әкімшінің жұмыс станциясында басқару плагиндері орнатылған бағдарламалардың атаулары ғана берілген.

  Егер бағдарлама таңдалмаса, онда өлшемшарт қолданылмайды.

- **Бағдарламаның нұсқасы**

  Енгізу өрісінде Kaspersky бағдарламасы нұсқасының нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер нұсқа нөмірі көрсетілмесе, онда өлшемшарт қолданылмайды.

- **Критикалық жаңартудың атауы**

  Енгізу өрісінде бағдарлама үшін белгіленген жаңарту пакетінің атауы немесе нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер өріс толтырылмаса, онда өлшемшарт қолданылмайды.

- **Модульдердің соңғы рет жаңартылған уақыты**

  Бұл параметрдің көмегімен құрылғыларда орнатылған бағдарлама модульдерінің соңғы рет жаңартылған уақыты бойынша құрылғыларды іздеу өлшемшартын белгілеуге болады.

  Егер жалауша қойылса, енгізу өрістерінде құрылғыларда орнатылған бағдарлама модульдерінің соңғы жаңартылуы орындалған аралық мәндерін (күні мен уақыты) көрсетуге болады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Құрылғы Kaspersky Security Center арқылы басқарылады**

  Ашылмалы тізімде Kaspersky Security Center басқаратын құрылғыларды таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама Kaspersky Security Center басқаратын құрылғыларды таңдауды қамтиды.
  - **Жоқ**. Қолданба Kaspersky Security Center арқылы басқарылмайтын құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қауіпсіздік бағдарламасы орнатылған**

  Ашылмалы тізімде қауіпсіздік бағдарламасы орнатылған құрылғыны таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама, қауіпсіздік бағдарламасы орнатылған құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қауіпсіздік қолданбасы орнатылмаған барлық құрылғыны таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Операциялық жүйе

Операциялық жүйе қойыншасында, орнатылған операциялық жүйе негізінде құрылғыларды іздеудің келесі өлшемшарттарын конфигурациялауға болады:

- **Операциялық жүйенің нұсқасы**

  Егер жалауша қойылса, тізімнен операциялық жүйелерді таңдауға болады. Көрсетілген операциялық жүйелер орнатылған құрылғылар іздеу нәтижелеріне қосылады.

- **Операциялық жүйенің биттік өлшемі**

  Ашылмалы тізімде операциялық жүйенің биттік өлшемін таңдауға болады, оның болуы бойынша құрылғыға құрылғыны жылжыту ережесі қолданылады (**Белгісіз**, **x86**, **AMD64** немесе **IA64**). Әдепкі бойынша, тізімде бірде-бір нұсқа таңдалмаған, операциялық жүйенің биттік өлшемі белгіленбеген.

- **Операциялық жүйенің қызметтік бума нұсқасы**

  Бұл өрісте операциялық жүйенің пакет нұсқасын (*X.Y* форматында) көрсетуге болады, ол жылжыту ережесінің құрылғыға қалай қолданылатынын анықтайды. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **Операциялық жүйе құрастырылымы**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйенің құрастыру нөмірі. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық құрастыру нөмірлерін іздеуді конфигурациялауға болады.

- **Операциялық жүйе шығарылымының идентификаторы**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйе шығарылымының идентификаторы. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш шығарылым идентификаторы болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық шығарылым идентификаторы нөмірлерін іздеуді конфигурациялауға болады.

Құрылғының күйі

Құрылғының күйі қойыншасында, басқарылатын бағдарламадан құрылғының күйі бойынша құрылғыларды іздеу өлшемшарттарын көрсетуге болады:

- **Құрылғының күйі**

  Құрылғы күйлерінің бірін таңдауға болатын ашылмалы тізім: *ОК*, *Критикалық* немесе *Ескерту*.

- **Нақты уақыт режимінде қорғау күйі**

  Нақты уақыт режимінде қорғау тапсырмасы күйінің мәнін таңдауға болатын ашылмалы тізім. Нақты уақыт режимінде қорғау күйі көрсетілген құрылғылар таңдауға қосылады.

- **Құрылғы күйінің сипаттамасы**

  Бұл өрісте орындалса, құрылғыға келесі күйлердің бірін тағайындайтын шарттардың жанындағы құсбелгі ұяшықтарын таңдай аласыз: *ОК, Критикалық* немесе *Ескерту*.

- **Бағдарлама анықтаған құрылғы күйі**

  Нақты уақыт режимінде қорғау тапсырмасы күйінің мәнін таңдауға болатын ашылмалы тізім. Нақты уақыт режимінде қорғау күйі көрсетілген құрылғылар таңдауға қосылады.

Қорғаныс компоненттері

Қорғаныс компоненттері қойыншасында клиент құрылғыларын іздеу параметрлерін қорғаныс күйіне қарай конфигурациялауға болады.

- **Дерекқорлардың шығарылған күні**

  Осы параметр таңдалса, клиент құрылғыларын іздеу антивирустық дерекқордың шығарылу күні бойынша орындалады. Енгізу өрістерінде іздеу жүргізілетін уақыт аралығын белгілеуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Вирустарға соңғы рет тексеру уақыты**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу соңғы рет зиянды БҚ іздеу уақыты бойынша жүзеге асырылады. Енгізу өрістерінде зиянды БҚ іздеу соңғы рет жүргізілген аралықты көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Анықталған қауіптердің жалпы саны**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу табылған вирустар санына сәйкес жүзеге асырылады. Енгізу өрістерінде табылған вирустар санының төменгі және жоғарғы мәндерін орнатуға болады.

  Әдепкі бойынша, параметр өшірулі.

Бағдарламалар тізімдемесі

Бағдарламалар тізімдемесі қойыншасында құрылғыларды іздеу параметрлерін оларда қандай бағдарламалар орнатылғанына байланысты конфигурациялауға болады:

- **Бағдарлама атауы**

  Бағдарламаны таңдауға болатын ашылмалы тізім. Көрсетілген бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарламаның нұсқасы**

  Таңдалған бағдарламаның нұсқасын көрсететін енгізу өрісі.

- **Өндіруші**

  Құрылғыда орнатылған бағдарламаның өндірушісін таңдауға болатын ашылмалы тізім.

- **Бағдарлама күйі**

  Бағдарлама күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған бағдарлама орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Жаңарту бойынша іздеу**

  Егер бұл параметр қосулы болса, іздеу сіз іздеген құрылғыларда орнатылған бағдарламаларды жаңарту деректері бойынша орындалады. Жалауша қойылғаннан кейін, **Бағдарлама атауы**, **Бағдарламаның нұсқасы** және **Бағдарлама күйі** өрістерінің орнына сәйкесінше **Жаңартудың атауы**, **Жаңартудың нұсқасы** және **Күйі** өрістері көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Үйлесімді емес қауіпсіздік бағдарламасының атауы**

  Үшінші тарап қауіпсіздік бағдарламаларын таңдауға болатын ашылмалы тізім. Іздеу кезінде, таңдалған бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарлама тегі**

  Ашылмалы тізімнен бағдарлама тегін таңдауға болады. Сипаттамада таңдалған тегі бар бағдарламалар орнатылған барлық құрылғылар құрылғылар таңдауына қосылады.

Басқару серверлерінің иерархиясы

Қосалқы Басқару серверлерінде сақталатын ақпараттың құрылғыларды іздеу кезінде ескерілуін, ал енгізу өрісінде құрылғыларды іздеу кезінде ақпарат ескерілетін қосалқы Басқару серверін енгізу деңгейінің көрсетілуін қаласаңыз, **Басқару серверлерінің иерархиясы** қойыншасында **Қосалқы Басқару серверлерінен деректерді қамту (келесі деңгейге дейін)** жалаушасын қойыңыз. Әдепкі бойынша, жалауша алынып тасталған.

Виртуалды машиналар

Виртуалды машиналар қойыншасында, құрылғылардың виртуалды машиналар немесе виртуалды жұмыс үстелдері инфрақұрылымының (VDI) бөлігі екендігіне байланысты, бұл құрылғыларды іздеу параметрлерін конфигурациялауға болады:

- **Виртуалды машина болып табылады**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Маңызды емес**.
  - **Жоқ**. Виртуалды машиналар емес құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

  Ашылмалы тізімнен виртуалды машина өндірушісін таңдауға болады.

  Бұл ашылмалы тізім **Виртуалды машина болып табылады** ашылмалы тізімінде **Иә** немесе **Маңызды емес** мәні таңдалған болса қолжетімді.

- **Virtual Desktop Infrastructure бөлігі**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Маңызды емес**.
  - **Жоқ**. Virtual Desktop Infrastructure-дың бөлігі болып табылмайтын құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар Virtual Desktop Infrastructure (VDI) бөлігі болуы тиіс.

Жабдық

Жабдық қойыншасында клиент құрылғыларын оларға орнатылған жабдық бойынша іздеуді конфигурациялауға болады:

- **Құрылғы**

  Ашылмалы тізімнен жабдық түрін таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Өндіруші**

  Ашылмалы тізімнен жабдық өндірушісінің атауын таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Сипаттама**

  Құрылғының немесе жабдықтың сипаттамасы. Өрісте көрсетілген сипаттамасы бар құрылғылар таңдау құрамына енгізіледі.

  Құрылғының сипаттамасын құрылғының сипаттары терезесінде еркін түрде енгізуге болады. Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Қойма нөмірі**

  Өрісте көрсетілген қойма нөмірі бар жабдық таңдауға қосылады.

- **Орталық процессор жиілігі, МГц түрінде**

  Орталық процессор жиіліктері ауқымы. Енгізу өрістеріндегі (қоса алғанда) жиіліктер ауқымына сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Орталық процессордың виртуалды ядролар саны**

  Орталық процессордың виртуалды ядролар саны ауқымы. Енгізу өрістеріндегі (қоса алғанда) ауқымға сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Қатты дискінің көлемі, ГБ түрінде**

  Құрылғының қатты дискісі көлемі мәндерінің ауқымы. Енгізу өрістеріндегі (қоса алғанда) ауқымға сәйкес келетін қатты дискілері бар құрылғылар таңдау құрамына енгізіледі.

- **Жедел жадтың көлемі, МБ түрінде**

  Құрылғының ЖЖҚ өлшеміне арналған мәндер ауқымы. Осы енгізу өрістеріндегі (инклюзивті) ауқымға сәйкес келетін ЖЖҚ-сы бар құрылғылар таңдауға қосылады.

Осалдықтар мен жаңартулар

Осалдықтар мен жаңартулар қойыншасында, Windows Update жаңарту көзі бойынша құрылғыларды іздеу өлшемшарттарын конфигурациялауға болады:

- **WUA Басқару серверіне ауысты**

  Ашылмалы тізімнен келесі іздеу нұсқаларының бірін таңдауға болады:

  - **Иә**. Егер бұл нұсқа таңдалса, іздеу нәтижелеріне Windows Update жаңартуларын Басқару серверінен алатын құрылғылар кіреді.

  - **Жоқ**. Бұл нұсқа таңдалса, нәтижелер жаңартуларды Windows Update арқылы басқа дереккөздерден алатын құрылғыларды қамтиды.

Пайдаланушылар

Пайдаланушылар қойыншасында, операциялық жүйеге кірген пайдаланушылардың есептік жазбалары бойынша құрылғыларды іздеу параметрлерін конфигурациялауға болады.

- **Жүйеге соңғы кірген пайдаланушы**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде пайдаланушы есептік жазбасын көрсетуге болады. Іздеу нәтижелеріне, жүйеге соңғы рет кіруді көрсетілген пайдаланушы орындаған құрылғылар кіреді.

- **Жүйеге кемінде бір рет кірген пайдаланушы**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде пайдаланушы есептік жазбасын көрсетуге болады. Іздеу нәтижелеріне, аталған пайдаланушы жүйеге кемінде бір рет кірген құрылғылар кіреді.

Басқарылатын бағдарламалардағы күйге әсер ететін мәселелер

Басқарылатын бағдарламалардағы күйге әсер ететін мәселелер қойыншасында, басқарылатын бағдарламадан құрылғылар күйлерінің сипаттамалары бойынша конфигурациялауға болады:

- **Құрылғы күйінің сипаттамасы**

  Сіз басқарылатын бағдарламалар күйлерінің сипаттамасы үшін жалаушаларды қоя аласыз, оларды алған кезде құрылғылар таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген күйді таңдағанда, сізде барлық тізімдерде осы күйді автоматты түрде таңдау мүмкіндігі болады.

Басқарылатын бағдарламалардың құрамдастарының күйлері

Басқарылатын бағдарламалардың құрамдастарының күйлері қойыншасында, басқарылатын бағдарламалардың құрамдастарының күйлері бойынша іздеуді конфигурациялауға болады:

- **Деректердің жайылып кетуіне жол бермеу күйі**

  Деректердің жайылып кетуінен қорғау құрамдасының күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Бірлескен жұмыс серверлерінің қорғаныс күйі**

  Бірлескен жұмыс серверлері үшін қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз*, *Тоқтатылды*, *Іске қосылды, Кідіртілді*, *Орындалуда*, *Сәтсіз аяқталды*).

- **Пошталық серверлердің антивирустық қорғаныс күйі**

  Пошта серверінің қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Endpoint Sensor күйі**

  Құрылғыларды Endpoint Sensor құрамдасының күйі бойынша іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

Шифрлау

- **Шифрлау**

  Advanced Encryption Standard (AES) симметриялық блоктық шифрлау алгоритмі стандарты. Ашылмалы тізімнен шифрлау кілтінің өлшемін таңдай аласыз (56 Бит, 128 Бит, 192 Бит немесе 256 Бит).

  Қолжетімді мәндер: *AES56*, *AES128*, *AES192*, және *AES256*.

Бұлттық сегменттер

Бұлттық сегменттер қойыншасында бұлттық сегменттерге тиесілілік бойынша іздеуді конфигурациялауға болады:

- **Құрылғы бұлттық сегментте орналасқан**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде іздеу сегментін көрсетуге болады.

  Қосалқы нысандарды қосу параметрі де қосулы болса, іздеу көрсетілген сегменттің барлық салынған нысандары бойынша жүргізіледі.

  Іздеу нәтижелеріне тек таңдалған сегменттегі құрылғылар кіреді.

- **Құрылғы API арқылы табылды**

  Ашылмалы тізімнен, құрылғының API құралдарымен анықталады ма екенін таңдауға болады:

  - **AWS**. Құрылғы AWS API арқылы табылды, яғни құрылғы AWS бұлтты ортасында орналасқан.
  - **Azure**. Құрылғы Azure API арқылы табылды, яғни құрылғы Azure бұлтты ортасында орналасқан.
  - **Google Cloud.** Құрылғы Google API арқылы табылды, яғни құрылғының Google Cloud ортасында орналасқаны анық.
  - **Жоқ**. Құрылғыны AWS, Azure немесе Google API пайдалану арқылы анықтау мүмкін емес, яғни ол бұлттық ортадан тыс немесе бұлттық ортада, бірақ оны API арқылы анықтау мүмкін емес.
  - **Көрсетілмеген**. Бұл шарт қолданылмайды.

Бағдарлама құрамдастары

Бұл бөлімде Басқару консолінде орнатылған тиісті басқару плагиндері бар бағдарламалар құрамдастарының тізімі келтірілген.

Бағдарлама құрамдастары қойындысында таңдалған қолданбаға қатысты құрамдастар күйлері мен нұсқа нөмірлеріне сәйкес құрылғыларды таңдауға қосу шарттарын көрсетуге болады.

- **Күйі**

  Басқарылатын бағдарлама Басқару серверіне жіберген құрамдастың күйіне сәйкес құрылғыларды іздеу. Сіз келесі күйлердің бірін таңдай аласыз: *Құрылғыдан деректер жоқ*, *Тоқтатылды*, *Іске қосылды*, *Кідіртілді*, *Орындалуда*, *Сәтсіз аяқталды* немесе *Орнатылмаған*. Егер басқарылатын құрылғыда орнатылған бағдарламаның таңдалған құрамдасы көрсетілген күйге ие болса, құрылғы құрылғыны таңдауға кіреді.

  Бағдарламалар жіберген күйлер:

  - *Іске қосылды* – құрамдас қазіргі уақытта инициализация процесінде.
  - *Орындалуда* – құрамдас қосулы және дұрыс жұмыс істейді.
  - *Кідіртілді* – құрамдас, мысалы, пайдаланушы басқарылатын бағдарламада қорғанысты кідірткеннен кейін кідіртіледі.
  - *Сәтсіз аяқталды* – құрамдастың операциясын орындау кезінде қате пайда болды.
  - *Тоқтатылды* – құрамдас өшірілген және қазіргі уақытта жұмыс істемейді.
  - *Орнатылмаған* – пайдаланушы бағдарламаны іріктеп орнату кезінде орнату құрамдасын таңдамады.

  Басқа күйлерден айырмашылығы: *Құрылғыдан келген деректер жоқ* күйін қолданбалар жібермейді. Бұл параметр, бағдарламаларда таңдалған құрамдас күйі туралы ақпарат жоқ екенін көрсетеді. Мысалы, бұл жағдай, таңдалған құрамдас құрылғыда орнатылған бағдарламалардың ешқайсысына тиесілі болмаса немесе құрылғы өшірулі болса, орын алуы мүмкін.

- **Нұсқа**

  Тізімде таңдалған құрамдас нұсқасының нөміріне сәйкес құрылғыларды іздеу. Сіз `3.4.1.0` сияқты нұсқа нөмірін енгізе аласыз, содан кейін таңдалған құрамдастың тең, анағұрлым ерте немесе анағұрлым кейінгі нұсқасы болуы керек пе екенін көрсете аласыз. Сондай-ақ, іздеуді көрсетілген нұсқадан басқа құрамдастың барлық нұсқалары бойынша конфигурациялауға болады.

Жол айнымалыларында бүркемелерді қолдану

Жол айнымалылары үшін бүркеніштерді қолдануға рұқсат етіледі. Бүркеніштер жасау үшін келесі тұрақты тіркестерді қолдануға болады:

- Алмастыру белгісі (*) – ұзындығы 0 немесе одан көп таңбадан тұратын кез келген жол.
- Сұрақ белгісі (?) – кез келген бір таңба.
- [<аралық>] – Берілген ауқымнан немесе жиынтықтан бір таңбаны ауыстырады.

  Мысалы: [0-9] - кез келген сан. [abcdef] – a, b, c, d, e, f таңбаларының бірі.

Іздеу жолында тұрақты өрнектерді қолдану

Бөлек сөздер мен таңбаларды іздеу үшін сіз іздеу жолында келесі тұрақты өрнектерді қолдана аласыз:

- *. Таңбалардың кез келген санының бірізділігін ауыстырады. Мысалы, "Сервер" немесе "Серверлік" сөздерін іздеу үшін іздеу жолында `Server*` өрнегін енгізу керек.
- ?. Кез келген бір таңбаны ауыстырады. Мысалы, "Құралдар" немесе "Құралдан" сөздерін іздеу үшін іздеу жолында `Құралда?` немесе өрнегін енгізу керек.

  > Іздеу жолындағы мәтін ? таңбасынан бастала аламайды.

- [<аралық>]. Белгіленген диапазон немесе жиын ішінен бір таңбаны ауыстырады. Мысалы, кез келген санды іздеу үшін іздеу жолында `[0-9]` өрнегін енгізу керек. a, b, c, d, e, f таңбаларының бірін іздеу үшін іздеу жолында `[abcdef]` өрнегін енгізу керек.

Толық мәтін бойынша іздеу үшін іздеу жолында келесі тұрақты өрнектерді қолдана аласыз:

- Бос орын. Нәтиже: сипаттамалары кез келген атап көрсетілген сөздерді қамтитын барлық құрылғылар. Мысалы, "Қосалқы" немесе "Виртуалды" сөзін (немесе олардың екеуін де) қамтитын сөйлемшені іздеу үшін, іздеу жолында `Қосалқы Виртуалды` өрнегін енгізу керек.
- "плюс" (+), AND немесе && белгісі. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болуын білдіреді. Мысалы, "Қосалқы" сөзін де, "Виртуалды" сөзін де қамтитын сөйлемшені іздеу үшін, іздеу жолында келесі өрнектерді енгізуге болады: `+Қосалқы+Виртуалды`, `Қосалқы AND Виртуалды`, `Қосалқы && Виртуалды`.
- OR немесе ||. Сөздердің арасында жазған кезде мәтіндің бір немесе басқа сөздің болуын білдіреді. "Қосымша" немесе "Виртуалды" сөзін қамтитын фразаны іздеу үшін іздеу өрісіне келесі өрнектердің кез келгенін енгізуге болады: `Қосымша НЕМЕСЕ виртуалды`, `Қосымша || виртуалды`.

- "минус" (-) белгісі. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болмауын білдіреді. Мысалы, "Қосалқы" сөзі болуы және "Виртуалды" сөзі болмауы тиісті сөйлемшені іздеу үшін, іздеу жолында `+Қосалқы-Виртуалды` өрнегін енгізу керек.

- `"<мәтін үзіндісі>"`. Тырнақшаға алынған мәтін үзіндісі мәтінде толығымен болуы керек. Мысалы, "Қосалқы Сервер" сөзтіркесін қамтитын сөйлемшені іздеу үшін іздеу жолында `"Қосалқы Сервер"` өрнегін енгізу керек.

Толық мәтін бойынша іздеу келесі сүзгілеу блоктарында қолжетімді:

- **Оқиға** және **Сипаттама** бағандары бойынша оқиғалар тізімін сүзгілеу блогында;

- **Атауы** бағаны бойынша пайдаланушылардың есептік жазбаларын сүзгілеу блогында;

- **Тізімде көрсету** блогында **топтаусыз** сүзгілеу өлшемшарты таңдалған болса, **Атауы** бағаны бойынша бағдарламалар тізімдемесін сүзгілеу блогында.

Диалог терезелеріндегі тізімдерді экспорттау

Бағдарлама тілқатысу терезелерінде сіз мәтіндік файлдарға нысан тізімдерін экспорттай аласыз.

Нысандар тізімін экспорттау **Файлға экспорттау** түймесі бар тілқатысу терезесінің бөлімдері үшін мүмкін.

Тапсырма параметрлері

Бұл бөлімде Kaspersky Security Center тапсырмаларының параметрлері атап көрсетілген.

Тапсырмалардың жалпы параметрлері

Бұл бөлім көптеген тапсырмаларыңыз үшін көруге және конфигурациялауға болатын параметрлердің сипаттамасын қамтиды. Қолжетімді параметрлердің тізімі конфигурацияланатын тапсырмаға байланысты.

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- Операциялық жүйені қайта жүктеу параметрлері:

  - **Құрылғыны қайта іске қоспау**

    Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сұрауды қайталау жиілігі (мин)**

  Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

- **Келесі уақыттан кейін қайта іске қосу (мин)**

  Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

- Тапсырма кестесі параметрлері:

  > Тапсырмаға байланысты кесте түрлері әртүрлі болуы мүмкін.

  - **Кесте бойынша іске қосу параметрлері:**

    - **N сағат сайын**

      Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

- **N күн сайын**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **Апта күндері бойынша**

  Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Бір рет**

  Тапсырма көрсетілген күн мен уақытта тек бір рет орындалады (тапсырманың жасалған күніне сәйкес).

- **Дереу**

  Тапсырма параметрлері сақталғаннан кейін бірден орындалады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Қоймаға жаңартуларды жүктеу кезінде**

  Бұл тапсырма жаңартуларды қоймаға жүктегеннен кейін іске қосылады. Мысалы, сізге осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін осы кесте қажет болуы мүмкін.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға ретсіз кідірісті қолдану аралығы (мин)**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- Тапсырма белгіленетін құрылғыларды таңдау терезесі:

  - **Басқару серверімен анықталған желілік құрылғыларды таңдау**

    Бұл жағдайда, тапсырма арнайы құрылғыларға тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

    Мысалы, сіз бұл параметрді Желілік агентті тағайындалмаған құрылғыларға орнату тапсырмасында пайдалана аласыз.

  - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

    Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

    Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

  - **Құрылғы таңдауына тапсырманы белгілеу**

    Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

    Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

  - **Басқару тобына тапсырманы белгілеу**

    Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

    Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

    Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

- Есептік жазба параметрлері:

  - **Әдепкі есептік жазба**

    Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **Есептік жазбаны көрсету**

    Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

  - **Есептік жазба**

    Тапсырманы іске қосатын есептік жазба.

  - **Құпиясөз**

    Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

> Егер мақсатты құрылғыда желілік агент орнатылмаған болса, admin$ бөлісу орнына қол жеткізу үшін мақсатты құрылғыда пайдаланылатын есептік жазбаны көрсету керек. Сіз көрсеткен есептік жазба деректерді құрылғыңызға көшіруге ғана арналған. Егер мақсатты құрылғыда желілік агент орнатылған болса, деректер желілік агент арқылы көшіріледі және тапсырманы жасау кезінде ешқандай есептік жазба көрсетудің қажеті жоқ.

Тапсырма жасалғаннан кейін белгіленген параметрлер

Тапсырманы жасағаннан кейін ғана келесі параметрлерді белгілеуге болады.

- Топтық тапсырма параметрлері:

  - **Ішкі топтарға тарату**

    Бұл параметр тек топтық тапсырмалардың сипаттарында қолжетімді.

    Бұл параметр қосылған кезде, тапсырманың әрекет ету ауқымы мыналарды қамтиды:

    - тапсырманы жасау кезінде сіз таңдаған басқару тобы;
    - топтар иерархиясы бойынша кез келген деңгейде таңдалған басқару тобына бағынатын басқару топтары.

    Егер бұл параметр өшірулі болса, тапсырманың құрамына тапсырманы жасау кезінде таңдаған басқару тобы ғана кіреді.

    Әдепкі бойынша, параметр қосулы.

  - **Қосалқы және виртуалды Басқару серверлеріне тарату**

    Бұл параметрді қосқан кезде, негізгі Басқару серверінде жұмыс істейтін тапсырма қосалқы (соның ішінде виртуалды) Басқару серверлерінде қолданылады. Егер Қосалқы Басқару серверінде бірдей типтегі тапсырма бұрыннан бар болса, онда қосалқы Басқару серверінде екі тапсырма да қолданылады — қолданыстағы және негізгі Басқару серверінен қабыл алынған.

    Ішкі топтарға тарату параметрі қосулы болса, бұл параметр қолжетімді болады.

Әдепкі бойынша, параметр өшірулі.

- Кестенің қосымша параметрлері:
  - **Тапсырманы бастамас бұрын, Желі арқылы қашықтан қосу технологиясы арқылы құрылғыларды іске қосу (мин)**

    Егер жалауша қойылса, құрылғыдағы операциялық жүйе тапсырма басталғанға дейін көрсетілген уақытта жүктеледі. Әдепкі бойынша белгіленген уақыт – 5 минут.

    Тапсырманы тапсырмалар аймағындағы барлық клиент құрылғыларында, соның ішінде тапсырма басталғалы тұрған кезде өшірілген құрылғыларда орындағыңыз келсе, осы параметрді қосыңыз.

    Тапсырманы орындағаннан кейін құрылғыны автоматты түрде өшіру қажет болса, **Тапсырманы орындағаннан кейін құрылғыларды өшіру** опциясын қосыңыз. Параметр сол терезеде орналасқан.

    Әдепкі бойынша, параметр өшірулі.

  - **Тапсырманы орындағаннан кейін құрылғыларды өшіру**

    Мысалы, жұмыс уақытынан кейін жұма сайын клиент құрылғыларына жаңартуларды орнататын, содан кейін демалыс күндері сол құрылғыларды өшіретін жаңартуларды орнату тапсырмасы үшін осы параметрді қосуға болады.

    Әдепкі бойынша, параметр өшірулі.

  - **Тапсырма мынанша минуттан көбірек орындалып жатса, оны тоқтату (мин)**

    Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

    Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

    Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.

- Хабарландыру параметрлері:
  - **Тапсырмалар журналын сақтау** блогы:
    - **Басқару серверінде мынанша (күн) бойы**

      Тапсырма аймағындағы барлық клиент құрылғыларында тапсырманы орындаумен байланысты бағдарлама оқиғалары көрсетілген күндер ішінде Басқару серверінде сақталады. Осы кезеңнен кейін ақпарат Басқару серверінен жойылады.

      Әдепкі бойынша, параметр қосулы.

    - **Құрылғыдағы ОЖ оқиғалар журналында сақтау**

      Тапсырманы орындауға байланысты, бағдарлама оқиғалары әрбір клиент құрылғысының Windows оқиғалар журналында жергілікті түрде сақталады.

      Әдепкі бойынша, параметр өшірулі.

- **Басқару серверіндегі ОЖ оқиғалар журналында сақтау**

  Тапсырма аймағындағы барлық клиент құрылғыларында тапсырманы орындаумен байланысты бағдарлама оқиғалары Басқару серверінің операциялық жүйесінің Windows оқиғалар журналында орталықтандырылған түрде сақталады.

  Әдепкі бойынша, параметр өшірулі.

- **Барлық оқиғаларды сақтау**

  Егер бұл параметр таңдалса, тапсырмаға қатысты оқиғалардың барлығы оқиғалар журналына жазылады.

- **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**

  Егер бұл параметр таңдалса, оқиғалар журналына тек тапсырманы орындаумен байланысты оқиғалар жазылады.

- **Тек тапсырманы орындау нәтижелерін сақтау**

  Егер бұл параметр таңдалса, оқиғалар журналына тек тапсырманы орындау нәтижелерімен байланысты оқиғалар жазылады.

- **Әкімшіге тапсырманы орындау нәтижелері туралы хабарлау**

  Сіз әкімшілердің тапсырманы орындау нәтижелері туралы хабар алу жолдарын таңдай аласыз: электрондық пошта, SMS арқылы және орындалатын файлды іске қосу кезінде. Хабарландыру параметрлерін конфигурациялау үшін **Параметрлер** сілтемесі арқылы өтіңіз.

  Барлық хабарландыру тәсілдері әдепкі бойынша өшірілген.

- **Тек қателер туралы хабарлау**

  Егер бұл параметр қосылса, әкімшілер тапсырма қате аяқталған жағдайда ғана хабарландыру алады.

  Егер бұл параметр өшірулі болса, әкімшілер тапсырма аяқталғаннан кейін хабарландыру алады.

  Әдепкі бойынша, параметр қосулы.

- Қауіпсіздік параметрлері

- Тапсырманың әрекет ету ауқымының параметрлері

  Тапсырманың әрекет ету ауқымы қалай анықталатынына байланысты келесі параметрлер бар:

  - **Құрылғылар**

    Егер тапсырманың әрекет ету ауқымы басқару топтарымен анықталса, сіз сол топты қарай аласыз. Мұнда ешқандай өзгерістер қолжетімді емес. Алайда, сіз **Тапсырма ауқымынан шығарып тастау** конфигурациялай аласыз.

    Егер тапсырманың әрекет ету ауқымы құрылғылар тізімімен анықталса, бұл тізім құрылғыларды қосу және жою арқылы өзгертілуі мүмкін.

  - **Құрылғыны таңдау**

    Тапсырма қолданылатын құрылғылар таңдауын өзгертуге болады.

- **Тапсырма ауқымынан шығарып тастау**

  Тапсырма қолданылмайтын құрылғылар тобын көрсетуге болады. Шығарылатын топтар тек тапсырма қолданылатын басқару тобының ішкі топтары бола алады.

- **Тексерістер журналы**

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы параметрлері

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- **Жаңартулардың көздері**

  Басқару сервері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:

  - Kaspersky жаңартулар серверлері

    Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері. Әдепкі бойынша, Басқару сервері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

    Әдепкі бойынша таңдалған.

  - Негізгі Басқару сервері

    Бұл ресурс қосалқы немесе виртуалды Басқару сервері үшін жасалған тапсырмаларға қатысты қолданылады.

  - Жергілікті немесе желілік қалта

    Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін. Желілік қалта түпнұсқалықты тексеруді қажет етсе, тек SMB протоколына қолдау көрсетіледі. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

    > Жаңарту көзі ретінде пайдаланылатын FTP серверінде, HTTP серверінде немесе желілік қалтада Kaspersky жаңарту серверлерін пайдалану кезінде жасалған қалталар құрылымына сәйкес келетін қалталар құрылымы (жаңартулармен бірге) болуы керек.

- **Басқа параметрлер**

  Қосалқы Басқару серверлерін мәжбүрлеп жаңарту

  Параметр қосылса, Басқару сервері жаңартуларды алғаннан кейін бірден бағыныңқы Басқару серверлерінде жаңартуларды алу тапсырмаларын іске қосады. Жаңарту тапсырмалары Басқару серверлеріндегі тапсырма сипаттамаларында конфигурацияланған жаңарту көзі арқылы іске қосылады.

  Егер бұл параметр өшірулі болса, қосалқы Басқару серверлеріндегі жаңарту тапсырмалары кестеге сәйкес басталады.

  Әдепкі бойынша, параметр өшірулі.

Алынған жаңартуларды қосымша қалталарға көшіру

Егер жалауша қойылса, жаңартуларды алғаннан кейін, Басқару сервері жаңартуларды көрсетілген қалталарға көшіреді. Құрылғыңыздағы жаңартуларды қолмен басқарғыңыз келсе, осы параметрді пайдаланыңыз.

Мысалы, сіз бұл параметрді келесі жағдайда пайдалана аласыз: ұйым желісінде бірнеше тәуелсіз ішкі желілер бар және әр ішкі желідегі құрылғылар басқа ішкі желіге қатынаса алмайды. Бұл жағдайда, барлық ішкі желілердегі құрылғылар ортақ желілік қалтаға қатынаса алады. Бұл жағдайда, ішкі желілердің біріндегі Басқару сервері үшін Kaspersky жаңарту серверлерінен жаңартуларды жүктеуді көрсетіңіз, осы параметрді қосыңыз және осы желілік қалтаны көрсетіңіз. Басқару сервері үшін жаңартуларды қоймаға жүктеу тапсырмасында дәл осы желілік қалтаны жаңартулар көзі ретінде көрсетіңіз.

Жүктелген жаңартуларды жергілікті қалтаға көшіруді таңдасаңыз, құрылғыда Басқару сервері орнатылған қалтаны көрсетуіңіз керек. Қалтаға апаратын жол құрылғының амалдық жүйесіне байланысты. Жергілікті қалта Linux негізіндегі Басқару серверінде орналасқандықтан, POSIX жолын көрсету керек, мысалы: /path/to/dir.

Linux негізіндегі Басқару серверінде орналасқан желілік қалтаны таңдағанда, қалтаны іске қосу арқылы Басқару сервері орнатылған құрылғыдан желілік қалтаға қатынасуды алдын ала қамтамасыз ету керек. Қалтаға қатынасу SMB протоколы арқылы жүзеге асырылады.

Әдепкі бойынша, параметр өшірулі.

Көшіру аяқталғанша құрылғыларды және қосалқы Басқару серверлерін мәжбүрлеп жаңартпау

Егер жалауша қойылса, клиент құрылғылары және қосалқы Басқару серверлері тарапынан жаңартуларды алу тапсырмалары, жаңартуларды желілік жаңартулар қалтасынан қосымша жаңартулар қалталарына көшіру аяқталғаннан кейін іске қосылады.

Егер клиент құрылғылары мен қосалқы Басқару серверлері жаңартуларды қосымша желілік қалталардан жүктесе, бұл жалауша қойылуы керек.

Әдепкі бойынша, параметр өшірулі.

Тапсырма жасалғаннан кейін белгіленген параметрлер

Тапсырманы жасағаннан кейін ғана келесі параметрлерді белгілеуге болады.

- **Параметрлер** бөлімі, **Жаңартулар мазмұны** блогы

  diff файлдарды жүктеп алу

  Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартуды тексеру** бөлімі

  Тарату алдында жаңартулар бар-жоғын тексеруді орындау

  Егер жалауша қойылса, Басқару сервері жаңартуларды көзден көшіреді, оларды уақытша қоймада сақтайды және **Жаңартуларды тексеру тапсырмасы** өрісінде көрсетілген Жаңартуларды тексеру тапсырмасын іске қосады. Бұл тапсырма сәтті орындалған жағдайда, жаңартулар уақытша қоймадан Басқару серверінің ортақ қатынас бар қалтасына көшіріледі және Басқару сервері жаңартулардың көзі болып табылатын құрылғыларға таратылады (**Қоймаға жаңартуларды жүктеу кезінде** кесте түрі бар тапсырмалар іске қосылады). Жаңартуларды қоймаға жүктеу тапсырмасы, тек *Жаңартуларды тексеру* тапсырмасы аяқталғаннан кейін аяқталған болып саналады.

Әдепкі бойынша, параметр өшірулі.

Жаңартуларды тексеру тапсырмасы

Бұл тапсырма, жаңарту көзі ретінде Басқару сервері таңдалған барлық құрылғыларға таратпас бұрын, жүктелген жаңартуларды тексереді.

Бұл өрісте, бұған дейін жасалған *Жаңартуларды тексеру* тапсырмасын көрсетуге болады. Сондай-ақ, сіз *Жаңартуларды тексеру* тапсырмасының басқасын жасай аласыз.

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасының параметрлері

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- **Жаңартулардың көздері**

  Тарату нүктелері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:

  - Kaspersky жаңарту серверлері

    Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

    Әдепкі бойынша, осы нұсқа таңдалады.

  - Негізгі Басқару сервері

    Бұл ресурс қосалқы немесе виртуалды Басқару сервері үшін жасалған тапсырмаларға қатысты қолданылады.

  - Жергілікті немесе желілік қалта

    Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін. Желілік қалта түпнұсқалықты тексеруді қажет етсе, тек SMB протоколына қолдау көрсетіледі. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

    > Жаңарту көзі ретінде пайдаланылатын FTP серверінде, HTTP серверінде немесе желілік қалтада Kaspersky жаңарту серверлерін пайдалану кезінде жасалған қалталар құрылымына сәйкес келетін қалталар құрылымы (жаңартулармен бірге) болуы керек.

- **Басқа параметрлер → Жаңартулар сақталатын қалта**

  Сақталған жаңартуларды сақтау үшін көрсетілген қалтаға апаратын жол. Көрсетілген қалтаға апаратын жолды алмасу буферіне көшіруге болады. Топтық тапсырма үшін көрсетілген қалтаға апаратын жолды өзгерте алмайсыз.

Тапсырма жасалғаннан кейін белгіленген параметрлер

Тапсырманы жасағаннан кейін ғана **Параметрлер** бөлімі, **Жаңартулар мазмұны** блогындағы келесі параметрлерді көрсете аласыз.

diff файлдарды жүктеп алу

Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

Әдепкі бойынша, параметр өшірулі.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- **Microsoft тізіміндегі осалдықтар мен жаңартуларды іздеңіз**

  Осалдықтар мен жаңартуларды іздеу кезінде Kaspersky Security Center бағдарламасы ағымдағы сәтте қолжетімді Microsoft жаңартулардың көздерінен Microsoft қолжетімді жаңартулары туралы деректерді қолданады.

  Мысалы, Microsoft жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

  - **Деректерді жаңарту үшін жаңарту серверіне қосылу**

    Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

    - Kaspersky Security Center Басқару сервері (Желілік агент саясатының параметрлерін қараңыз).
    - Ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server.
    - Microsoft жаңарту серверлері.

    Егер бұл параметр қосулы болса, басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылып, Microsoft Windows қолжетімді жаңартулары туралы ақпарат алады.

    Егер бұл параметр өшірулі болса, басқарылатын құрылғыдағы Windows Update агенті бұған дейін Microsoft жаңарту көзінен алған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты пайдаланады.

Microsoft жаңарту көзіне қосылу ресурстарды қажет етуі мүмкін. Егер сіз осы жаңарту көзіне басқа тапсырмада немесе Желілік агент саясатының сипаттарында, **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** бөлімінде тұрақты қосылым орнатқан болсаңыз, бұл параметрді өшіре аласыз Егер сіз бұл параметрді өшіргіңіз келмесе, Серверге түсетін жүктемені азайту үшін тапсырмалар кестесін 360 минут аралығындағы тапсырманы іске қосу кідірісінің кездейсоқ мәнін пайдалануға болатындай конфигурациялауға болады.

Әдепкі бойынша, параметр қосулы.

Желілік агент саясаты параметрлерінің келесі мәндерінің тіркесімі жаңартуларды алу режимін анықтайды:

- Басқарылатын құрылғыдағы Windows Update агенті жаңартуларды алу үшін жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының сипаттарында қосылған және **Windows Update жаңартуларын іздеу режимі** параметрі желілік агент саясатының параметрлерінде **Белсенді** болып белгіленген жағдайда ғана қосылады.

- *Осалдықты сканерлеу* тапсырмасын орындаған кезде Microsoft Windows жаңарту көзіне қосылымды бастау және жаңартуларды жүктеп алу үшін Желілік агент қажет болмаса, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатуға болады, бұл арада **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы күйде қала беруі керек. Бұл, ресурстарды үнемдеуге және осалдықтарды іздеу үшін бұрын алынған Windows жаңартуларын пайдалануға мүмкіндік береді. Microsoft Windows жаңартуларын алуды басқа тәсілмен конфигурациялаған болсаңыз, пассивті режимді пайдалануға болады. Microsoft Windows жаңартуларын басқа жолмен алу үшін конфигурацияланбасаңыз, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатпаңыз, себебі бұл жағдайда жаңартулар туралы ақпарат ешқашан алынбайды.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметріне қарамастан (қосулы немесе өшірулі), егер **Windows Update жаңартуларын іздеу режимі** параметрі үшін **Өшірулі** параметрлер тобында таңдалса, онда Kaspersky Security Center бағдарламасы жаңартулар туралы ақпаратты сұрамайды.

- **Kaspersky ұсынған үшінші тарап осалдықтары мен жаңартуларын іздеңіз**

  Егер бұл параметр қосулы болса, Kaspersky Security Center бағдарламасы Windows тізімдемесінде және **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз** бөлімінде көрсетілген қалталарда үшінші тарап өндірушілерінің бағдарламалары (Kaspersky және Microsoft-тан басқа өндірушілер шығарған бағдарламалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап бағдарламаларының толық тізімін Kaspersky бақылайды.

  Егер бұл параметр өшірулі болса, Kaspersky Security Center бағдарламасы үшінші тарап бағдарламалары үшін осалдықтар мен қажетті жаңартуларды іздемейді. Мысалы, Microsoft Windows жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

  - **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз**

    Kaspersky Security Center бағдарламасы осалдықтарды түзетуді және жаңартуларды орнатуды қажет ететін үшінші тарап бағдарламаларын іздейтін қалталар. Жүйе айнымалыларын пайдалануға болады.

    Бағдарламалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген бағдарламалар орнатылған жүйелік қалталар бар.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

  - **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

    Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы параметрлері

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- **Жаңа нұсқаларды орнатуға арналған ережелерді көрсетіңіз**

  Бұл ережелер клиент құрылғыларына жаңартуларды орнату кезінде қолданылады. Егер ережелер көрсетілмесе, тапсырма орындалмайды. Ережелермен жұмыс істеу туралы қосымша ақпаратты Жаңартуларды орнату ережелері бөлімінен қараңыз.

- **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау**

  Егер жалауша қойылса, құрылғыны қайта іске қоспас немесе өшірмес бұрын жаңартуды орнату орындалады. Әйтпесе, жаңартуларды орнату кесте бойынша жүзеге асырылады.

  Жаңартуларды орнату құрылғылардың жұмысына әсер етуі мүмкін болса, осы жалаушаны қойыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Қажетті жалпы жүйелік құрамдастарды орнату**

  Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

  Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартулар кезінде бағдарламаның жаңа нұсқаларын орнатуға рұқсат ету**

  Бұл опция қосылған болса, бағдарламалық жасақтама қолданбасының жаңа нұсқасын орнатуға әкелсе, жаңартуларға рұқсат беріледі.

  Бұл параметр өшірулі болса, бағдарлама жаңартылмайды. Бағдарламалардың жаңа нұсқаларын кейінірек қолмен немесе басқа тапсырманы қолдана отырып, орнатуға болады. Мысалы, егер сіздің компанияңыздың инфрақұрылымы бағдарламаның жаңа нұсқасын қолдамаса немесе сынақ инфрақұрылымындағы жаңартуды тексеру қажет болса, бұл параметрді пайдалануға болады.

  Әдепкі бойынша, параметр қосулы.

  > Бағдарламаның жаңа нұсқасын орнатқаннан кейін, клиент құрылғыларында орнатылған және жаңартылатын бағдарламаның жұмысына байланысты басқа бағдарламалардың жұмысы бұзылуы мүмкін.

- **Жаңартуларды құрылғыға орнатпастан жүктеп алу**

  Егер жалауша қойылса, бағдарлама жаңартуларды құрылғыға жүктейді, бірақ оларды автоматты түрде орнатпайды. Содан кейін, жүктелген жаңартуларды қолмен орнатуға болады.

  Microsoft жаңартулары Windows қызметтік қалтасына жүктеледі. Үшінші тарап бағдарламаларының жаңартулары (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) **Жаңартуларды келесі жерге жүктеп алу** өрісінде көрсетілген қалтаға жүктеледі.

  Егер бұл параметр өшірулі болса, жаңартулар құрылғыға автоматты түрде орнатылады.

  Әдепкі бойынша, параметр өшірулі.

  - **Жаңартуларды келесі жерге жүктеп алу**

    Бұл қалта, үшінші тарап бағдарламаларының (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) жаңартуларын жүктеу үшін қолданылады.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

  - **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

    Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

Тапсырма жасалғаннан кейін белгіленген параметрлер

Төменде келтірілген параметрлерді тапсырма жасалғаннан кейін ғана орнатуға болады. Тапсырма параметрлерінің толық сипаттамасын Тапсырмалардың жалпы параметрлері бөлімінен қараңыз.

- **Жалпы**. Бұл бөлімде тапсырма туралы жалпы ақпарат көрсетіледі. Сондай-ақ, қандай құрылғыларға *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы қолданылуы керектігін көрсетуге болады:

  - **Ішкі топтарға тарату**

    Бұл параметр тек топтық тапсырмалардың сипаттарында қолжетімді.

    Бұл параметр қосылған кезде, тапсырманың әрекет ету ауқымы мыналарды қамтиды:

    - тапсырманы жасау кезінде сіз таңдаған басқару тобы;
    - топтар иерархиясы бойынша кез келген деңгейде таңдалған басқару тобына бағынатын басқару топтары.

    Егер бұл параметр өшірулі болса, тапсырманың құрамына тапсырманы жасау кезінде таңдаған басқару тобы ғана кіреді.

    Әдепкі бойынша, параметр қосулы.

  - **Қосалқы және виртуалды Басқару серверлеріне тарату**

    Бұл параметрді қосқан кезде, негізгі Басқару серверінде жұмыс істейтін тапсырма қосалқы (соның ішінде виртуалды) Басқару серверлерінде қолданылады. Егер Қосалқы Басқару серверінде бірдей типтегі тапсырма бұрыннан бар болса, онда қосалқы Басқару серверінде екі тапсырма да қолданылады — қолданыстағы және негізгі Басқару серверінен қабыл алынған.

    Ішкі топтарға тарату параметрі қосулы болса, бұл параметр қолжетімді болады.

    Әдепкі бойынша, параметр өшірулі.

- Орнатылатын жаңартулар

  Орнатылатын жаңартулар бөлімінде тапсырмада белгіленген жаңартулар тізімін көруге болады. Таңдалған тапсырманың параметрлеріне сәйкес келетін жаңартулар ғана көрсетіледі.

- Жаңартуларды сынап орнату:

  - **Сканерлемеу**. Жаңартуларды тексеріп орнатқыңыз келмесе, осы нұсқаны таңдаңыз.
  - **Таңдалған құрылғыларда сканерлеуді іске қосу**. Белгілі бір құрылғыларда жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Қосу** түймесін басып, жаңартуларды тексеріп орнату қажет құрылғыларды таңдаңыз.
  - **Көрсетілген топтағы құрылғыларда сканерлеуді іске қосу**. Құрылғылар тобында жаңартуларды орнатуды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Сынақ топты белгілеңіз** өрісінде тексеріп орнату қажет құрылғылар тобын көрсетіңіз.
  - **Құрылғылардың көрсетілген пайызында сканерлеуді іске қосу**. Құрылғылардың бөліктеріне жаңартуларды тексергіңіз келсе, осы нұсқаны таңдаңыз. **Құрылғылардың жалпы санынан сынақ құрылғылардың пайызы** өрісінде жаңартуларды тексеріп орнату қажет құрылғылар пайызын көрсетіңіз.

Глобалды қосалқы желілердің тізімі

Бұл бөлімде, ережелерде қолдануға болатын глобалды қосалды желілердің тізімі туралы ақпарат келтірілген.

Желіңіздің ішкі желілері туралы ақпаратты сақтау үшін, сіз әрбір Басқару сервері үшін глобалды қосалқы желілердің тізімін конфигурациялай аласыз. Бұл тізім филиалдардың кеңселері сияқты физикалық бірліктер мен жұптарды (IP мекенжайы, бүркеніш) салғастыруға мүмкіндік береді. Сіз желілік ережелер мен параметрлердегі тізімнен ішкі желілерді қолдана аласыз.

Глобалды қосалқы желілердің тізіміне ішкі желіні қосу

Ішкі желілер мен олардың сипаттамасын глобалды қосалқы желілердің тізіміне қоса аласыз.

Глобалды қосалқы желілердің тізіміне ішкі желіні қосу үшін:

1. Консоль ағашында Басқару серверінің қажетті түйінін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Глобалды қосалқы желілердің тізімі** бөлімін таңдаңыз.
4. **Қосылуда** түймесін басыңыз.

   Жаңа ішкі желі терезесі ашылады.
5. Келесі өрістерді толтырыңыз:

   - **Жалпы параметрлер**

     Сіз қосатын ішкі желінің IP мекенжайы.

   - **Ішкі желі маскасы**

     Сіз қосатын ішкі желінің бүркеніші.

   - **Атауы**

     Ішкі желі атауы. Ішкі желі атауы барлық глобалды қосалқы желілердің тізімі үшін бірегей болуы керек. Тізімде бұрыннан бар ішкі желі атауын көрсеткен болсаңыз, оған индекс қосылады, мысалы: ~~1, ~~2.

   - **Сипаттама**

     Сипаттамасында қосымша ақпарат, мысалы, осы ішкі желі тиесілі болып табылатын филиал туралы ақпарат болуы мүмкін. Бұл мәтін, ішкі желілер тізімі көрсетілетін барлық жерде, мысалы, трафикті шектеу ережелері тізімінде туындайды.

     Бұл өріс толтыру үшін міндетті емес және бос қалдырылуы мүмкін.
6. **OK** түймесін басыңыз.

Ішкі желі ішкі желілер тізімінде пайда болады.

Глобалды қосалқы желілердегі ішкі желінің сипаттарын қарау және өзгерту

Глобалды қосалқы желілердің тізімінде ішкі желілердің сипаттарын қарап, өзгерте аласыз.

Глобалды қосалқы желілердің тізімінде ішкі желінің сипаттарын қарау немесе өзгерту үшін:

1. Консоль ағашында Басқару серверінің қажетті түйінін таңдаңыз.
2. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
3. **Бөлімдер** панелінде ашылған **Сипаттар** терезесінде **Глобалды қосалқы желілердің тізімі** бөлімін таңдаңыз.
4. Тізімнен қажетті ішкі желіні таңдаңыз.
5. **Сипаттар** түймесін басыңыз.

   Жаңа ішкі желі терезесі ашылады.
6. Қажет болса, ішкі желі параметрлерін өзгертіңіз.
7. **ОК** түймесін басыңыз.

Өзгерістер жасаған болсаңыз, олар сақталады.

Желілік агентті Windows, Linux және macOS үшін қолдану: салыстыру

Желілік агентті пайдалану құрылғының операциялық жүйесіне байланысты. Желілік агент саясатының және орнату пакетінің сипаттары операциялық жүйеге байланысты. Төмендегі кестеде Windows, macOS және Linux операциялық жүйелері үшін қолжетімді Желілік агентінің мүмкіндіктері мен пайдалану сценарийлері салыстырылады.

Желілік агент функцияларын салыстыру

Желілік агент функциясы	Windows	Linux	macOS
Орнату			
Kaspersky Security Center орнатқаннан кейін, Желілік агенттің орнату пакетін автоматты түрде құру	✓	–	–
Kaspersky Security Center бағдарламаларын қашықтан орнату тапсырмасының тиісті параметрлерінің көмегімен мәжбүрлеп орнату.	✓	✓	✓
Пайдаланушыларға Kaspersky Security Center қалыптастырған автономды пакеттерге сілтемелер тарату арқылы бағдарламалар орнату.	✓	✓	✓

Желілік агент функциясы	Windows	Linux	macOS
Қатты дискінің кескінін операциялық жүйемен және орнатылған Желілік агентпен, диск кескіндерімен жұмыс істеу үшін Kaspersky Security Center ұсынатын құралдармен бірге клондау арқылы орнату	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Операциялық жүйесі мен Желілік агенті бар әкімші қатты дискісі кескінін үшінші тарап құралдарымен клондау әдісімен орнату	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Бағдарламаларды қашықтан орнатудың үшінші тарап құралдары арқылы бағдарламалар орнату	✓	✓	✓
Құрылғыларда бағдарлама инсталляторларын іске қосу арқылы қолмен орнату	✓	✓	✓
Желілік агентті тыныш режимде орнату	✓	✓	✓
Клиент құрылғысын Басқару серверіне қолмен қосу	✓	✓	✓
Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнату	✓	✓	—
Кілтті автоматты түрде тарату	✓	✓	✓
Мәжбүрлеп синхрондау	✓	✓	✓ Push серверінен басқа
Тарату нүктесі			
Тарату нүктесін қолдану	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Тарату нүктелерінің саны мен конфигурациясын есептеу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓ Network Location Awareness (NLA) қолданбай.	✓ Network Location Awareness (NLA) қолданбай.
Желіде сауалнама өткізу	✓ • Windows желісінің сауалнамасы • IP ауқымдарының сауалнамасы • Домен контроллерлеріне сауалнама жүргізу (Microsoft Active Directory) Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓ • IP ауқымдарының сауалнамасы • Zeroconf сауалнамасы • Домен контроллерлерінің сауалнамасы (Microsoft Active Directory, Samba 4 Active Directory)	—

Желілік агент функциясы	Windows	Linux	macOS
KSN прокси-сервері қызметін тарату нүктесінің жағында іске қосу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	—
Жаңартуларды басқарылатын құрылғыларға тарататын тарату нүктесі қоймаларына Kaspersky жаңарту серверлері арқылы жүктеп алу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	— Linux немесе macOS операциялық жүйесі бар құрылғылар Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасының әрекет ету ауқымында болса, онда тапсырма Windows операциялық жүйесі бар құрылғылардың барлығында сәтті аяқталса да, Сәтсіз аяқталды мәртебесімен аяқталады.
Бағдарламаларды күшпен орнату	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	Шектеумен: Linux операциялық жүйесі бар тарату нүктелерін қолдана отырып, Windows операциялық жүйесі басқаратын құрылғыларда күшпен орнату мүмкін емес.	Шектеумен: macOS операциялық жүйесі бар тарату нүктелерін қолдана отырып, Windows операциялық жүйесі басқаратын құрылғыларда күшпен орнату мүмкін емес.
Push-сервер ретінде қолдану	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	—
Үшінші тарап бағдарламаларымен жұмыс істеу			
Бағдарламаларды құрылғыларға қашықтан орнату	✓	—	✓ Мәліметтер алу үшін келесі мақаланы қараңыз: Қолданбаларды macOS құрылғыларына қашықтан орнату.
Бағдарламалық жасақтама жаңартуы	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Желілік агент саясатында операциялық жүйенің жаңартуларын конфигурациялау	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Бағдарламалық жасақтама осалдықтарын іздеу	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	—	—
Құрылғыларда орнатылған бағдарламалық жасақтаманы түгендеу	✓	✓	—
Виртуалды машиналар			
Виртуалды машиналарға Желілік агент орнату	✓	✓	✓

Желілік агент функциясы	Windows	Linux	macOS
VDI үшін параметрлерді оңтайландыру	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Динамикалық виртуалды машиналарды қолдау	✓ Шектеу: Arm жүйесіндегі Microsoft Windows жүйесіне арналған Желілік агент қолдамайды.	✓	✓
Басқа			
Windows компьютерлік бөлісу қызметі арқылы қашықтағы клиент құрылғысындағы әрекеттер аудиті	✓	—	—
Антивирустық қорғаныс күйі мониторингі	✓	✓	✓
Құрылғыларды қайта іске қосуды басқару	✓	—	—
Файлдық жүйені шегіндіруді қолдау	✓	✓	✓
Желілік агентті қосылым шлюзі ретінде пайдалану	✓	✓	✓
Байланыс менеджері	✓	✓	✓
Желілік агентті бір Басқару серверінен екіншісіне ауыстырып қосу (автоматты түрде желілік орналасуы бойынша)	✓	—	✓
Клиент құрылғысы мен басқару сервері арасындағы қосылымды тексеру. klnagchk утилитасы	✓	✓	✓
Клиент құрылғысының жұмыс үстеліне қашықтан қосылу	✓	—	✓ Virtual Network Computing (VNC) жүйесін пайдалану.
Деректерді тасымалдау шебері арқылы жеке орнату пакетін жүктеу	✓	✓	✓
Zeroconf сауалнамасы	—	✓	—
Клиент құрылғыларының аппараттық жасақтамасы туралы ақпаратты қарау	✓	✓ Осы құрылғыларда орнатылған желілік агент арқылы басқару серверіне жіберілген Linux құрылғыларының аппараттық жасақтамасы туралы ақпарат басқару консолі және Kaspersky Security Center Web Console бойынша басқарылатын құрылғы параметрлерінің сипаттамасында көрсетілген ақпаратпен шектеледі.	✓ Осы құрылғыларда орнатылған желілік агент арқылы басқару серверіне жіберілген macOS құрылғыларының аппараттық жасақтамасы туралы ақпарат басқару консолі және Kaspersky Security Center Web Console бойынша басқарылатын құрылғы параметрлерінің сипаттамасында көрсетілген ақпаратпен шектеледі.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console бағдарламасы, Kaspersky бағдарламалары қорғайтын ұйым желілерінің қауіпсіздік жүйесінің күйін бақылауға арналған бағдарлама (веб-қолданба) болып табылады.

Бағдарламаның көмегімен сіз келесі әрекеттерді орындай аласыз:

- Ұйымыңыздың қауіпсіздік жүйесінің күйін бақылай аласыз.
- Kaspersky бағдарламаларын желіңіздің құрылғыларына орната аласыз және орнатылған бағдарламаларды басқара аласыз.
- Желіңіздің құрылғылары үшін құрастырылған саясаттарды басқара аласыз.
- Пайдаланушы есептік жазбаларын басқара аласыз.
- Желінің құрылғыларына орнатылған бағдарламалардың тапсырмаларын басқара аласыз.
- Қауіпсіздік жүйесінің күйлері туралы есептерді қарай аласыз.
- Мүдделі тұлғаларға: жүйелік әкімшілер мен басқа да IT мамандарына есептерді жеткізуді басқара аласыз.

Аппараттық және бағдарламалық құрал талаптарын Web Console веб консолінің талаптарын қараңыз.

Kaspersky Security Center Web Console бағдарламасы браузер арқылы Басқару серверімен өзара әрекеттесуді қамтамасыз ететін веб-интерфейс болып саналады. Басқару сервері – бұл сіздің желіңіздің құрылғыларына орнатылған Kaspersky бағдарламаларын басқаруға арналған бағдарлама. Басқару сервері сіздің желіңіздің құрылғыларымен қорғалған (SSL) байланыс арналары арқылы байланысады. Сіз браузер арқылы Kaspersky Security Center Web Console серверіне қосылған кезде, браузер Kaspersky Security Center Web Console серверімен қорғалған (HTTPS) қосылымды орнатады.

Kaspersky Security Center Web Console сервері келесідей жұмыс істейді:

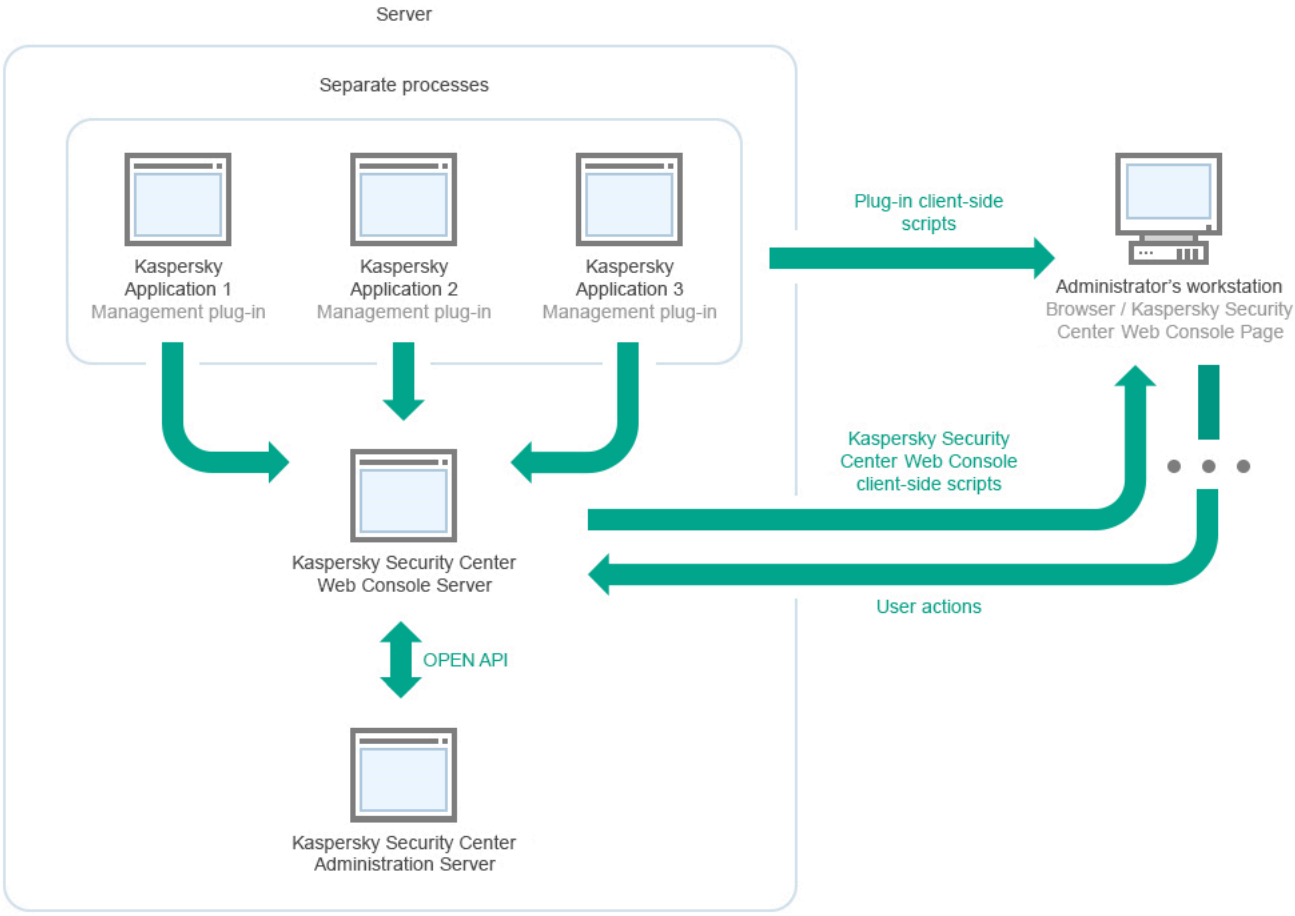
1. Сіз Kaspersky Security Center Web Console серверіне бағдарламаның веб-порталының беттерін көрсететін браузер арқылы қосыласыз.
2. Веб-порталдың басқару элементтерінің көмегімен, орындағыңыз келетін пәрменді таңдайсыз. Kaspersky Security Center Web Console сервері келесі әрекеттерді орындайды:
   - Ақпарат алумен байланысты пәрменді таңдаған болсаңыз (мысалы, құрылғылар тізімін қарау), Kaspersky Security Center Web Console бағдарламасы Басқару серверіне ақпарат алу туралы сұрау салып, одан қажетті деректерді алады және оларды браузерге көрсету үшін ыңғайлы түрде жібереді.
   - Басқару пәрменін таңдаған болсаңыз (мысалы, бағдарламаны қашықтан орнату), онда Kaspersky Security Center Web Console бағдарламасы браузерден пәрмен алып, оны Басқару серверіне жібереді. Содан кейін, бағдарлама Басқару серверінен пәрменнің орындалу нәтижесін алады және нәтижені көрсетуге ыңғайлы түрде браузерге жібереді.

Kaspersky Security Center Web Console көп тілді бағдарлама болып саналады. Бағдарламаны қайта ашпай-ақ интерфейс тілін кез келген уақытта өзгертуге болады. Егер сіз Kaspersky Security Center Web Console бағдарламасын Kaspersky Security Center-мен бірге орнатсаңыз, Kaspersky Security Center Web Console бағдарламасы орнату файлымен бірдей интерфейс тіліне ие. Егер сіз тек Kaspersky Security Center Web Console орнатсаңыз, бағдарлама операциялық жүйемен бірдей тілге ие. Егер Kaspersky Security Center Web Console бағдарламасы орнату файлының немесе операциялық жүйенің тілін қолдамаса, онда ағылшын тілі әдепкі бойынша орнатылады.

Kaspersky Security Center Web Console бағдарламасында ұялы құрылғыларды басқаруға қолдау көрсетілмейді. Алайда, егер сіз Басқару консолиндегі басқару тобына ұялы құрылғыларды қосқан болсаңыз, бұл құрылғылар Kaspersky Security Center Web Console бағдарламасында да көрсетіледі.

Kaspersky Security Center Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы

Келесі суретте Kaspersky Security Center Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы келтірілген.



Kaspersky Security Center Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орналастыру схемасы

Қорғалатын құрылғыларда орнатылған Kaspersky бағдарламаларын басқару плагиндерін (әр бағдарлама үшін бөлек плагин) орналастыру Kaspersky Security Center Web Console серверін орналастырумен бір мезгілде жүзеге асырылады.

Әкімші ретінде, сіз Kaspersky Security Center Web Console бағдарламасына өзіңіздің жұмыс станцияңыздың браузері арқылы қатынаса аласыз.

Сіз Kaspersky Security Center Web Console бағдарламасында белгілі бір әрекеттерді орындаған кезде, Kaspersky Security Center Web Console сервері Kaspersky Security Center Басқару серверімен OpenAPI арқылы өзара әрекеттеседі. Kaspersky Security Center Web Console сервері Kaspersky Security Center Басқару серверінен қажетті деректерді сұрайды және Kaspersky Security Center Web Console бағдарламасында сіздің әрекеттеріңіздің нәтижелерін көрсетеді.

Kaspersky Security Center Web Console бағдарламасы қолданатын порттар

Төмендегі кестеде Kaspersky Security Center Web Console Server сервері (бұдан әрі жай ғана Kaspersky Security Center Web Console) орнатылған құрылғыда ашылатын порттар тізімі атап көрсетілген.

Kaspersky Security Center Web Console бағдарламасы қолданатын порттар

Порт нөмірі	Қызмет атауы	Протокол	Портты тағайындау	Аймақ
2001	Kaspersky Security Center Product Plugins Server	HTTPS	Kaspersky Security Center Web Console Management Service қызметінен сұрауларды қабылдау үшін басқару плагин процестері тарапынан қолданылатын API порт	Басқару плагиндерінің node.exe процестерін іске қосу
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	Бір құрылғыда жұмыс істейтін Kaspersky Security Center Web Console Management Service қызметінен сұрауларды қабылдау үшін пайдаланылатын API порттар	Kaspersky Security Center Web Console құрамдастарын жаңарту
2005	Kaspersky Security Center Web Console	HTTPS	Бір құрылғыда жұмыс істейтін Kaspersky Security Center Web Console Management Service қызметінен сұрауларды қабылдау үшін пайдаланылатын API порт.	Kaspersky Security Center Web Console веб-консолін орнатуды бастау
3333	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 соңғы авторизация нүктесі порты	Есептік деректер және қатынасу диспетчері
4004	Kaspersky OSMP Facade Service	HTTPS	OAuth2.0 идентификация провайдері порты	Есептік деректер және қатынасу диспетчері
4444	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 токенінің соңғы өзіндік талдау нүктесі порты	Есептік деректер және қатынасу диспетчері
8200	—	HTTP	HashiCorp Vault арқылы сертификаттар жасау үшін қолданылатын API порты (толық ақпарат HashiCorp Vault сайтында)	Kaspersky Security Center Web Console веб-консолін орнату және Kaspersky Security Center Web Console құрамдастарын жаңарту
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTPS	Kaspersky Security Center Web Console және басқару плагиндері арасындағы байланыс үшін пайдаланылатын Message Broker API порттары	Kaspersky Security Center Web Console және басқару плагиндері арасындағы өзара іс қимыл

Төмендегі кестеде Kaspersky Security Center Web Console сервері орнатылған құрылғыда міндетті түрде ашылмайтын порттар келтірілген. Алайда, Kaspersky Security Center Web Console сервері осы порттарды Есептік деректер және қатынасу диспетчері үшін қолданады.

Kaspersky Security Center Web Console тарапынан Есептік деректер және қатынасу диспетчері үшін қолданылатын порттар

Порт нөмірі	Қызмет атауы	Протокол	Портты тағайындау	Аймақ
4445	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 соңғы авторизация нүктесінің порты үшін Kaspersky Security Center Web Console серверінен конфигурацияны алатын Есептік деректер және қатынасу диспетчерінің негізгі порты (OAuth 2.0 туралы толық ақпарат OAuth веб-сайтында)	Есептік деректер және қатынасу диспетчері
2444	Kaspersky OSMP Facade Service	HTTPS	Есептік деректер және қатынасу диспетчері конфигурациялау порты	Есептік деректер және қатынасу диспетчері
2445	Kaspersky OSMP Facade Service	HTTPS	Kaspersky OSMP KAS Service қызметін Kaspersky OSMP Facade Service қызметіне қосу порты	Есептік деректер және қатынасу диспетчері

Kaspersky Security Center Web Console интерфейсі

Kaspersky Security Center жүйесі Kaspersky Security Center Web Console интерфейсі арқылы басқарылады.

Kaspersky Security Center Web Console қолданбасының терезесі келесі элементтерді қамтиды:

- Терезенің сол жағындағы негізгі мәзір
- Терезенің оң жағындағы жұмыс аймағы

Негізгі мәзір

Негізгі мәзір келесі бөлімдерден тұрады:

- **Басқару сервері**. Қазіргі уақытта қосылған Басқару серверінің атауын көрсетеді. Басқару сервері сипаттарын ашу үшін параметрлер белгішесін ( ) басыңыз.
- **Бақылау және есеп беру**. Желіңіздің инфрақұрылымы, қорғаныс күйі, сондай-ақ статистика туралы мәлімет береді.
- **Активтер (Құрылғылар)**. Құрамында активтерге арналған құралдар, сонымен қатар Kaspersky қолданбаларына арналған тапсырмалар мен саясаттар бар.
- **Пайдаланушылар және рөлдер**. Пайдаланушылар мен рөлдерді басқаруға, пайдаланушы құқықтарын конфигурациялауға, пайдаланушыларға рөлдерді тағайындауға және саясат профильдерін рөлдермен байланыстыруға мүмкіндік береді.
- **Операциялар**. Қолданбаны лицензиялау, шифрланған дискілерді және шифрлау оқиғаларын көру және басқару және үшінші тарап қолданбаларын басқару сияқты әртүрлі параметрлерді қамтиды. Бөлім, сонымен қатар, қолданбалар қоймаларына қол жеткізуге мүмкіндік береді.
- **Құрылғыларды табу және орналастыру**. Клиент құрылғыларын анықтау және құрылғыларды басқару топтарына қолмен немесе автоматты түрде тарату үшін желіде сауалнама жүргізуге мүмкіндік береді. Бұл бөлімде бастапқы орнату шебері және қорғанысты орналастыру шебері бар.
- **Marketplace**. Kaspersky бизнес-шешімдері туралы ақпаратты қамтиды, сізге қажет шешімдерді таңдауға және Kaspersky сайтында осы шешімдерді сатып алуды жалғастыруға мүмкіндік береді.

- **Параметрлер**. Сізге сақталған күйді қалпына келтіру үшін веб-плагиннің ағымдағы күйінің деректерін сақтық көшірмелеуге мүмкіндік береді. Интерфейс тілі немесе тақырыбы сияқты интерфейстің сыртқы түріне қатысты жеке параметрлерді қамтиды.

- **Есептік жазбаңыздың мәзірі**. Kaspersky Security Center анықтамасының сілтемесін қамтиды. Сондай-ақ, Kaspersky Security Center жүйесінен шығып, Kaspersky Security Center Web Console нұсқасын және орнатылған басқарудың веб-плагиндерінің тізімін көруге болады.

Жұмыс аймағы

Жұмыс аймағы Kaspersky Security Center Web Console интерфейсі терезесінің бөлімдерінде көру үшін таңдалған ақпаратты көрсетеді. Сондай-ақ, ол ақпаратты көрсетуді конфигурациялау үшін пайдалануға болатын басқару элементтерін қамтиды.

Негізгі мәзір бөлімдерін бекіту және бекітуді болдырмау

Kaspersky Security Center Web Console веб-консолі бөлімдерін таңдаулыларыңызға қосу және оларға негізгі мәзірдегі **Бекітілген** бөлімнен жылдам қол жеткізу үшін бекітуге болады.

> Бекітілген элементтер болмаса, негізгі мәзірде **Бекітілген** бөлімі пайда болмайды.

Тек беттерді көрсететін бөлімдерді бекітуге болады. Мысалы, **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** тармағына өтсеңіз, құрылғылар кестесі бар бет ашылады, яғни **Басқарылатын құрылғылар** бөлімін бекітуге болады. Егер негізгі мәзірде бөлімді таңдағаннан кейін терезе көрсетілсе немесе элемент көрсетілмесе, онда мұндай бөлімді бекітуге болмайды.

Бөлімді бекіту үшін:

1. Негізгі мәзірден тінтуірді бекіткіңіз келетін бөлімнің үстіне апарыңыз.

   Бекіту белгішесі (📌) көрсетіледі.

2. Бекіту белгішесін (📌) басыңыз.

Бөлім бекітілген және **Бекітілген** бөлімде көрсетіледі.

Сондай-ақ, таңдаулылардан элементтерді бекітуді болдырмау арқылы жоюға болады.

Бөлімді бекітуді болдырмау үшін:

1. Қолданбаның негізгі терезесінде **Бекітілген** бөліміне өтіңіз.

2. Босату қажет бөлімнің үстіне тінтуір меңзерін апарып, босату белгішесін (📌) басыңыз.

Бөлім таңдаулылардан жойылды.

Kaspersky Security Center Web Console веб-консолін орнату және бастапқы конфигурациялау

Бұл бөлімде Kaspersky Security Center Басқару сервері мен Kaspersky Security Center Web Console бағдарламасын орнату, бағдарламаны жылдам іске қосу шебері арқылы Басқару серверін бастапқы конфигурациялау, сондай-ақ қорғанысты орналастыру шебері арқылы басқарылатын құрылғыларға Kaspersky бағдарламаларын орнату тәсілі сипатталған.

Kaspersky Security Center Web Console бағдарламасын орнату және бастапқы конфигурациялау келесі кезеңдерден тұрады:

1. **Дерекқорды басқару жүйесін (ДҚБЖ) орнату**

   ДҚБЖ, қолданылатын Kaspersky Security Center бағдарламасын орнатыңыз немесе қолданыстағы ДҚБЖ қолданыңыз.

   Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

2. **Басқару серверін, Басқару консолі, және Желілік агентті орнату**

   Басқару серверімен бірге Басқару консолі және Желілік агенттің серверлік нұсқасы да орнатылады.

   Kaspersky Security Center Басқару серверін орнату барысында дәл осы құрылғыға Kaspersky Security Center Web Console бағдарламасын орнату керек пе екенін көрсетуге болады. Егер сіз екі компонентті де бір құрылғыға орнатуды ұйғарсаңыз, онда сізге Kaspersky Security Center Web Console бағдарламасын бөлек орнатудың қажеті жоқ, себебі ол автоматты түрде орнатылады. Kaspersky Security Center Web Console бағдарламасын басқа құрылғыға орнатқыңыз келсе, онда Kaspersky Security Center Басқару серверін орнатқаннан кейін, Kaspersky Security Center Web Console орнатуға өтіңіз.

3. **Kaspersky Security Center Web Console орнату**

   Алдыңғы қадамда Kaspersky Security Center Басқару серверімен бірге Kaspersky Security Center Web Console бағдарламасын орнатуды таңдамаған болсаңыз, Kaspersky Security Center Web Console бағдарламасын басқа құрылғыда орнатыңыз. Kaspersky Security Center Web Console бағдарламасы, Басқару сервері орнатылған құрылғыдан ерекшеленетін құрылғыны орнатуға болады.

4. **Бастапқы конфигурациялауды орындау**

   Басқару серверін орнату аяқталғаннан кейін, Басқару серверіне алғаш рет қосылған кезде Бағдарламаны жылдам іске қосу шебері автоматты түрде іске қосылады. Сіздің талаптарыңызға сәйкес Басқару серверін бастапқы конфигурациялауды орындаңыз. Бағдарламаны жылдам іске қосу кезеңінде, шебер қорғанысты орналастыру үшін қажетті әдепкі бойынша параметрі бар саясат пен тапсырманы жасайды. Бұл параметрлер сіздің ұйымыңыздың қажеттіліктері үшін оңтайлы болмауы мүмкін. Қажет болса, саясаттар мен тапсырмалар параметрлерін өзгерте аласыз.

5. **Kaspersky Security Center лицензиялау (қажет болса)**

   Басқару консолінің негізгі функциясын қолдайтын Kaspersky Security Center үшін лицензия қажет емес. Осалдықтар мен патчтарды басқаруды, Ұялы құрылғыларды басқаруды және SIEM жүйелерімен біріктіруді қоса алғанда, бағдарламаның бір немесе бірнеше қосымша мүмкіндіктерін пайдаланғыңыз келсе, сізге коммерциялық лицензия қажет. Осы мүмкіндіктер үшін кілт файлын немесе белсендіру кодын бағдарламаны жылдам іске қосу шеберінің тиісті қадамында немесе қолмен қоса аласыз.

6. **Желілік құрылғыларды табу**

   Бұл кезеңді бағдарламаны жылдам іске қосу шебері өңдейді. Құрылғыларды табуды қолмен де орындауға болады. Нәтижесінде, Kaspersky Security Center Басқару сервері желіде тіркелген барлық құрылғылардың мекенжайлары мен атауларын алады. Алдағыда, Kaspersky Security Center көмегімен табылған құрылғыларға Kaspersky және басқа өндірушілердің бағдарламаларын орната аласыз. Kaspersky Security Center құрылғыларды анықтауды үнемі іске қосады, сондықтан желіде жаңа құрылғылар пайда болса, олар автоматты түрде анықталады.

7. **Құрылғыларды басқару топтарына біріктіру**

   Бұл қадамды бағдарламаны жылдам іске қосу шебері өңдейді, бірақ сіз табылған құрылғыларды басқару топтарына қолмен де жылжыта аласыз.

8. **Желідегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнату**

   Ұйымның желісінде қорғанысты орналастыру Желілік агент пен қауіпсіздік бағдарламаларын (мысалы, Kaspersky Endpoint Security for Windows) Басқару сервері құрылғыларды анықтау процесінде тапқан құрылғыларға орнатуды қамтиды.

   Бағдарламаны қашықтан орнатуды орындау үшін қорғанысты орналастыру шеберін іске қосыңыз.

   Қауіпсіздік бағдарламалары құрылғыларды вирустардан және басқа қауіп төндіретін бағдарламалардан қорғайды. Желілік агент құрылғының Басқару серверімен байланысын қамтамасыз етеді. Желілік агенттің параметрлері әдепкі бойынша автоматты түрде конфигурацияланады.

   Желідегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнатпас бұрын, бұл құрылғылардың қолжетімді (қосулы) екеніне көз жеткізіңіз.

9. **Лицензиялық кілттерді клиент құрылғыларына тарату**

   Осы құрылғыларда басқарылатын қауіпсіздік бағдарламаларын белсендіру үшін лицензиялық кілттерді клиент құрылғыларына таратыңыз.

10. **Kaspersky Security for Mobile орнату (міндетті емес)**

    Корпоративтік ұялы құрылғыларды басқаруды жоспарласаңыз, Kaspersky Endpoint Security for Android орналастыру туралы ақпарат алу үшін Kaspersky Security for Mobile анықтамасын қараңыз.

11. **Kaspersky бағдарламаларының саясаттарын конфигурациялау**

    Әртүрлі құрылғыларда бағдарламалардың әртүрлі параметрлері қолданылуы үшін, құрылғы қауіпсіздігін басқару немесе пайдаланушыға бағытталған қауіпсіздікті басқару нұсқаларын пайдалануға болады. Құрылғылардың қауіпсіздігін басқару саясаттар мен тапсырмалар арқылы іске асырылады. Тапсырмаларды тек белгілі бір шарттарға сәйкес келетін құрылғыларда орындауға болады. Құрылғы таңдаулары шарттарын жасау үшін құрылғы таңдаулары мен тегтер қолданылады.

12. **Желі қорғанысы күйінің мониторингі**

    Сіз ақпараттық тақтадағы веб-виджеттер арқылы желі жұмысын бақылауды ұйымдастыра аласыз, Kaspersky бағдарламалары туралы есептер жасай аласыз, басқарылатын құрылғылардағы бағдарламалардан алынған оқиғаларды таңдауды конфигурациялап, көре аласыз және хабарландырулар тізімін көре аласыз.

Орнату

Бұл бөлімде Kaspersky Security Center және Kaspersky Security Center Web Console бағдарламаларын орнату жолы сипатталған.

Kaspersky Security Center орнату (стандартты орнату)

Бұл бөлімде Kaspersky Security Center орнату тәсілі сипатталған. Алдымен дерекқорды басқару жүйесін орнату қажет.

Kaspersky Security Center орнату үшін:

1. Әкімші құқықтары бар есептік жазбамен ksc_<құрылым нөмірі>_full_<локализация тілі>.exe орындалатын файлын іске қосыңыз.
2. Ашылған қолданбаны таңдау терезесінде **Kaspersky Security Center орнату** түймесін басыңыз.

   Kaspersky Security Center басқару серверінің орнату шеберінің терезесі ашылады.
3. Сәлемдесу терезесінен бастап **Келесі** түймесін басу арқылы шебер қадамдарынан өтіңіз.
4. Ол орнатылмаған болса, Microsoft .NET Framework орнатыңыз.
5. Лицензиялық келісім мен Құпиялық саясатын қабылдаңыз.
6. Орнату түрін таңдаңыз. Ақпараттық мақсатта көрсетілген әдепкі түрді қалдыру ұсынылады: **Стандартты**.
7. Kaspersky Security Center Web Console консолін Kaspersky Security Center бар бір құрылғыға орнату қажет болса, **Kaspersky Security Center Web Console орнату** жалаушасын қойыңыз.

   Бұл жалауша қойылмаса, Kaspersky Security Center Web Console консолін сол не басқа құрылғыға бөлек орнатуға болады.
8. Желі өлшемін көрсетіңіз. Ақпараттық мақсаттар үшін көрсетілген әдепкі мәнді қалдыру ұсынылады: **100 желілік құрылғыдан аз**.
9. Бұрын орнатылған дерекқор серверінің түрін таңдаңыз.
10. Бұрын орнатылған дерекқор серверіне қосылу параметрлерін көрсетіңіз.
11. Бұрын орнатылған дерекқор сервері үшін аутентификация параметрлерін көрсетіңіз.
12. Орнатуды бастау үшін **Орнату** түймесін басыңыз.
13. Орнату сәтті аяқталғаннан кейін, шебер жұмысын аяқтағаннан кейін бірден басқару консолін іске қосқыңыз келетін-келмейтінін көрсетіңіз.

    Kaspersky Security Center Web Console ашуды таңдасаңыз, кіру экраны ашылады. Содан кейін бастапқы реттеу шеберін пайдаланып, басқару серверінің бастапқы реттеуін орындауға болады.

    Kaspersky Security Center Web Console орнатылған болса ғана, оны ашуға болады. Kaspersky Security Center орнатқан кезде Kaspersky Security Center Web Console орнатпасаңыз немесе бөлек орнатпасаңыз, оны ашу мүмкін емес.
14. Ашылған басқару консолі терезесінде орнатылған басқару серверін таңдаңыз.
15. Жалғастыру үшін басқару сервері сертификатымен ашылатын терезеде **Иә** түймесін басыңыз.

Басқару серверінің бастапқы орнату шебері басқару консолінің веб-нұсқасында іске қосылмаған болса, іске қосылады.

Ақаулықтарды жою

Басқару сервері сертификаты бар терезе көрсетілмесе және қосылым қатесі туралы хабарлар пайда болса:

1. Windows жүйесінде **Қызметтер** терезесін ашыңыз (**Басқару панелі** → **Басқару** → **Қызметтер**). Kaspersky Security Center желілік агенті және Kaspersky Security Center басқару сервері қызметтері іске қосылғанына көз жеткізіңіз.

2. Windows жүйесінде **Оқиғаларды көру** терезесін (**Басқару панелі** → **Басқару** → **Оқиғаларды көру**) ашып, **Қолданбалар мен қызметтер журналы** → **Kaspersky Event Log** тармағын таңдаңыз. Оқиғалар журналында қате жазбалары жоқ екеніне және **<нұсқа нөмірі> басқару сервері іске қосылған** түріндегі оқиғалар туралы жазбалар бар екеніне көз жеткізіңіз.

Kaspersky Security Center Web Console орнату

Бұл бөлімде Kaspersky Security Center Web Console серверін (бұдан әрі Kaspersky Security Center Web Console деп те аталады) қалай бөлек орнатуға болатыны сипатталған. Алдымен ДҚБЖ және Kaspersky Security Center басқару серверін орнату қажет. Kaspersky Security Center Web Console бағдарламасын, Kaspersky Security Center орнатылған құрылғыға немесе басқасына орната аласыз.

Kaspersky Security Center Web Console орнату үшін:

1. ksc-web-console-<нұсқа_нөмірі>.<жинақ нөмірі>.exe орнату файлын әкімші құқықтары бар есептік жазбамен іске қосыңыз.

   Орнату шебері іске қосылады.

2. Орнату шебері тілін таңдаңыз.

3. Сәлемдесу терезесінде **Келесі** түймесін басыңыз.

4. **Лицензиялық келісім** терезесінде Лицензиялық келісімді оқып, шарттарын қабылдаңыз. Орнату, Лицензиялық келісім қабылданғаннан кейін жалғасады, әйтпесе **Келесі** түймесі қолжетімді емес.

5. **Мақсатты қалта** терезесінде Kaspersky Security Center Web Console бағдарламасы орнатылатын қалтаны таңдаңыз (әдепкі бойынша %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Мұндай қалта болмаса, ол орнату барысында автоматты түрде жасалады.

   Сіз мақсатты қалтаны **Шолу** түймесі арқылы өзгерте аласыз.

6. **Kaspersky Security Center Web Console байланыс параметрлері** терезесінде келесі ақпаратты көрсетіңіз:

   - Kaspersky Security Center Web Console мекенжайы (әдепкі бойынша 127.0.0.1);
   - Kaspersky Security Center Web Console бағдарламасы кіріс қосылымдары үшін пайдаланатын порт, яғни Kaspersky Security Center Web Console-ге браузерден кіруге мүмкіндік беретін порт (әдепкі бойынша 8080).

   Әдепкі бойынша мекенжай мен порт мәндерін қалдыру ұсынылады.

   Таңдалған порттың қолжетімді ме екенін тексергіңіз келсе, **Сынақ** түймесін басыңыз.

   Kaspersky Security Center Web Console журналына жазбаны қосқыңыз келсе, тиісті параметрді таңдаңыз. Бұл параметр таңдалмаса, Kaspersky Security Center Web Console журналының файлдары жасалмайды.

7. **Есептік жазба параметрлері** терезесінде есептік жазбалар мен құпиясөздерді көрсетіңіз.

   Әдепкі бойынша есептік жазбалардың мәндерін пайдалану ұсынылады.

8. **Клиенттік сертификат** терезесінде келесі параметрлердің бірін таңдаңыз:

   - **Жаңа сертификатты құру**. Егер сізде браузер сертификаты болмаса, бұл нұсқаны пайдалану ұсынылады.

   - **Бұрыннан бар сертификатты таңдаңыз**. Сізде браузер сертификаты болса, осы опцияны таңдауға болады; бұл жағдайда оның жолын көрсетіңіз.

   - Егер сіз сертификат жасауды таңдасаңыз, Kaspersky Security Center Web Console бағдарламасын ашқан кезде, браузер сізге Kaspersky Security Center Web Console бағдарламасына қосылудың жекеше емес екенін және Kaspersky Security Center Web Console сертификаты жарамсыз екенін хабарлауы мүмкін. Бұл ескерту, Kaspersky Security Center Web Console сертификаты өздігінен қол қоятындықтан және оны Kaspersky Security Center автоматты түрде жасайтындықтан пайда болады. Осы ескертуді жою үшін, сіздің инфрақұрылымыңызда сенімді болып саналатын және пайдаланушы сертификаттарына қойылатын талаптарға сәйкес келетін сертификат жасаңыз. Содан кейін, **Бұрыннан бар сертификатты таңдаңыз** терезесінде **Клиенттік сертификат** параметрін таңдап, пайдаланушы сертификатыңызға апаратын жолды көрсетіңіз.

   PFX пішіміндегі сертификаттарға Kaspersky Security Center Web Console бағдарламасы қолдау көрсетпейді. Мұндай сертификатты пайдалану үшін, алдымен оны Windows операциялық жүйесіне арналған OpenSSL сияқты OpenSSL негізіндегі кроссплатформалық утилитаның көмегімен қолдау көрсетілетін PEM пішіміне түрлендіру қажет.

9. **Сенімді Басқару серверлері** терезесінде Басқару серверіңіздің тізімде екеніне көз жеткізіп, орнату шеберінің соңғы терезесіне өту үшін **Келесі** түймесін басыңыз.

   Тізімге жаңа Басқару серверін қосу қажет болса, **Қосу** түймесін басыңыз. Ашылған терезеде жаңа сенімді Басқару серверінің сипаттарын көрсетіңіз:

   - **Басқару серверінің атауы**

     Kaspersky Security Center Web Console веб-консоліне кіру терезесінде көрсетілетін Басқару серверінің атауы.

   - **Басқару серверінің мекенжайы**

     Басқару серверін орнатып жатқан құрылғының IP мекенжайы.

   - **Басқару серверінің порты**

     Kaspersky Security Center Web Console веб-консолі Басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі бойынша 13299).

   - **Басқару серверінің сертификаты**

     Сертификат файлы Басқару сервері орнатылған құрылғыда сақталады. Басқару серверінің сертификатына әдепкі бойынша апаратын жол:

     - Windows операциялық жүйесі бар құрылғылар үшін: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

     - Linux операциялық жүйесі бар құрылғылар үшін: /var/opt/kaspersky/klnagent_srv/1093/cert/.

Kaspersky Security Center Web Console веб-консолін Басқару сервері орнатылған құрылғыға орнатып жатсаңыз, жоғарыдағы жолдардың бірін пайдаланыңыз. Немесе Басқару сервері орнатылған құрылғыдан сертификат файлын Kaspersky Security Center Web Console орнатып жатқан құрылғыға көшіріп, сертификатқа жергілікті жолды көрсетіңіз.

10. **Есептік деректер және қатынасу диспетчері (IAM)** терезесінде Identity and Access Manager (бұдан әрі IAM деп те аталады) орнату керек пе екенін көрсетіңіз. Есептік деректер және қатынасу диспетчерін орнатуды таңдасаңыз, келесі порт нөмірлерін көрсетіңіз:

    - **KAS әкімші порты**. Әдепкі бойынша, 4445-порт OAuth2.0 авторизациясының соңғы нүктесі портына арналған Kaspersky Security Center Web Console конфигурациясын алу үшін пайдаланылады.
    - **Facade әкімші порты**. Әдепкі бойынша, 2444-порт Есептік деректер және қатынасу диспетчерін конфигурациялау үшін қолданылады.
    - **Facade өзара әрек. порты**. Әдепкі бойынша, 2445-порт Kaspersky OSMP KAS Service сервисін Kaspersky OSMP Facade Service сервисіне қосу үшін қолданылады.

    Сіз әдепкі бойынша порт нөмірлерін өзгерте аласыз. Болашақта сіз оларды Kaspersky Security Center Web Console арқылы өзгерте алмайсыз.

11. Орнату шеберінің соңғы терезесінде, орнатуды бастау үшін **Орнату** түймесін басыңыз.

Орнату сәтті аяқталғаннан кейін, жұмыс үстелінде таңбаша пайда болады және сіз Kaspersky Security Center Web Console бағдарламасына кіре аласыз.

Microsoft Management Console бағдарламасына кіріктірілген Басқару консолінде іске қосылмаған болса, Басқару серверін жылдам іске қосу шебері іске қосылады.

Ақаулықтарды жою

Kaspersky Security Center Web Console бағдарламасы браузеріңізде сіз көрсеткен мекенжай бойынша көрсетілмесе, келесі әрекеттерді орындап көріңіз:

1. Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғының көрсетілген атауының немесе IP мекенжайының дұрыстығын тексеріңіз.
2. Сіз жұмыс істеп жатқан құрылғының Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыға қатынаса алатынына көз жеткізіңіз.
3. Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғының желілік экран параметрлері 8080-порт арқылы және node.exe қолданбасы үшін кіріс қосылымдарына рұқсат беретініне көз жеткізіңіз.
4. Windows ОЖ-де **Қызметтер** терезесін ашыңыз. Kaspersky Security Center Web Console іске қосылғанына көз жеткізіңіз.
5. Басқару консолі арқылы Kaspersky Security Center бағдарламасына қатынаса алатыныңызға көз жеткізіңіз.
6. Windows операциялық жүйесінде **Оқиғаларды көру** терезесін ашып, **Қолданбалар мен қызметтер журналы → Kaspersky Event журналы** тармағын таңдаңыз. Оқиғалар журналында қателер туралы жазбалар жоқ екеніне көз жеткізіңіз.

Kaspersky істен шығуға төзімді кластерінің түйіндерінде орнатылған Басқару серверіне қосылған Kaspersky Security Center Web Console орнату

Бұл бөлімде ақауларға төзімді Kaspersky Security Center немесе ақауларға төзімді Windows Server кластерінің түйіндерінде орнатылған басқару серверіне қосылатын Kaspersky Security Center Web Console серверін (бұдан әрі — Kaspersky Security Center Web Console) орнату жолы сипатталған. Kaspersky Security Center Web Console серверін орнатпас бұрын, ДҚБЖ және Kaspersky Security Center басқару серверін ақауларға төзімді Kaspersky Security Center кластерінің түйіндеріне немесе ақауларға төзімді Windows Server кластерінің түйіндеріне орнатыңыз.

Ақауларға төзімді Windows Server кластерін пайдалансаңыз, Kaspersky Security Center Web Console серверін ақауларға төзімді кластер түйініне орнату ұсынылмайды. Түйін істен шыққан болса, сіз Басқару серверіне қатынасу құқығын жоғалтасыз.

Істен шығуға төзімді кластердің түйіндерінде орнатылған Басқару серверіне қосылатын Kaspersky Security Center Web Console веб-консолін орнату үшін:

1. 1-қадамнан 8-қадамға дейін Kaspersky Security Center Web Console веб-консолін орнату бөліміндегі қадамдарды орындаңыз.

2. Сенімді Басқару сервері ретінде ауыстырып қосу кластерін қосу үшін **Сенімді Басқару серверлері** терезесіндегі 9-қадамда **Қосу** түймесін басыңыз.

   Ашылған терезеде келесі параметрлерді көрсетіңіз:

   - **Басқару серверінің атауы**

     Kaspersky Security Center Web Console веб-консоліне кіру терезесінде көрсетілетін кластер атауы.

   - **Басқару серверінің мекенжайы**

     Істен шығуға төзімді кластердің түріне байланысты кластер мекенжайын көрсетіңіз:

     - **Ақауларға төзімді Kaspersky Security Center кластері**. Кластер түйіндерін дайындау кезінде адаптерді жасаған болсаңыз, қосымша желілік адаптердің IP мекенжайын кластер мекенжайы ретінде көрсетіңіз. Не болмаса, өзіңіз пайдаланып жатқан үшінші тарап теңгергішінің IP мекенжайын көрсетіңіз.

     - **Ақауларға төзімді Windows Server кластері**. Ақауларға төзімді Windows Server кластерін жасаған кезде алған кластер мекенжайын көрсетіңіз.

   - **Басқару серверінің порты**

     Kaspersky Security Center Web Console веб-консолі Басқару серверіне қосылу үшін пайдаланатын OpenAPI порты (әдепкі бойынша 13299).

- **Басқару серверінің сертификаты**

  Басқару серверінің сертификаты ақауларға төзімді Kaspersky Security Center кластерінің немесе ақауларға төзімді Windows Server кластерінің ортақ деректер қоймасында орналасқан. Сертификат файлына әдепкі бойынша жол: <ортақ деректер қалтасы>\1093\cert\klserver.cer. Сертификат файлын ортақ деректер қоймасынан Kaspersky Security Center Web Console орнатып жатқан құрылғыға көшіріңіз. Басқару серверінің сертификатына апаратын жергілікті жолды көрсетіңіз.

3. Kaspersky Security Center Web Console стандартты орнатуды жалғастырыңыз.

Сәтті аяқталғаннан кейін, жұмыс үстелінде таңбаша пайда болады және сіз Kaspersky Security Center Web Console бағдарламасына кіре аласыз.

Kaspersky Security Center Web Console жаңарту

Егер сіз Kaspersky Security Center Web Console серверінің қазіргі уақытта орнатылған үлгісін жоймай, жаңа нұсқасын пайдаланғыңыз келсе, онда Kaspersky Security Center Web Console орнатушысында қарастырылған стандартты жаңарту процедурасын пайдалана аласыз.

Kaspersky Security Center Web Console жаңарту үшін:

1. Әкімші құқықтары бар есептік жазбаның астында ksc-web-console-<нұсқа нөмірі>.<құрастыру нөмірі>.exe орындалатын файлын іске қосыңыз, мұндағы <құрастыру нөмірі> дегеніміз сіз орнатқан үлгіден үлкен нөмірі бар Kaspersky Security Center Web Console құрастыру нөмірін білдіреді.

2. Орнату шеберінің ашылған терезесінде тілді таңдап, **OK** түймесін басыңыз.

3. Сәлемдесу терезесінде **Жаңарту** параметрін таңдап, **Келесі** түймесін басыңыз.

4. **Лицензиялық келісім** терезесінде Лицензиялық келісімді оқып, шарттарын қабылдаңыз. Орнату, Лицензиялық келісім қабылданғаннан кейін жалғасады, әйтпесе **Келесі** түймесі қолжетімді емес.

5. Орнату аяқталмайынша, орнату шеберінің барлық қадамдарын орындаңыз. Орнату процесінде сіз алдыңғы орнату кезінде көрсеткен Kaspersky Security Center Web Console параметрлерін де өзгерте аласыз. **Kaspersky Security Center Web Console консолін өзгертуге дайын** қадамына жеткен кезде, **Жаңарту** түймесін басыңыз. Жаңа параметрлер күшіне енгенше күтіңіз және орнату шеберінің келесі қадамында **Аяқтау** түймесін басыңыз. Сондай-ақ, жаңартылған Kaspersky Security Center Web Console үлгісін дереу іске қосу үшін **Браузерде Kaspersky Security Center Web Console консолін іске қосу** сілтемесінен өтуге болады.

   > Жаңарту кезінде Kaspersky Security Center Web Console параметрлерін өзгерту тек Kaspersky Security Center 12.2 Web Console және одан жоғары нұсқаларында қолжетімді.

   Kaspersky Security Center Web Console бағдарламасы орнатылды.

Kaspersky Security Center Web Console веб-консолімен жұмыс істеуге арналған сертификаттар

Бөлімде Kaspersky Security Center Web Console сертификаттарын қалай шығару және ауыстыру керектігі, сондай-ақ Сервер Kaspersky Security Center Web Console веб-консолімен өзара әрекеттесетін болса, Басқару сервері сертификатын қалай жаңарту керектігі сипатталған.

Kaspersky Security Center Web Console үшін сертификатты қайта шығару

Көптеген браузерлер сертификаттың жарамдылық мерзімін шектейді. Бұл шектеуге кіру үшін Kaspersky Security Center Web Console сертификатының жарамдылық мерзімі 397 күнге тең. Жаңа өздігінен қол қойылған сертификатты қолмен шығарған кезде, сенімді сертификаттау орталығынан (CA) алынған қолданыстағы сертификатты ауыстыруға болады. Сондай-ақ, Kaspersky Security Center Web Console ескірген сертификатын қайта шығаруға болады.

> Kaspersky Security Center Web Console үшін сертификатты автоматты түрде қайта шығаруға қолдау көрсетілмейді. Сертификатты қолмен қайта шығаруыңыз керек.

Егер сіз қазірдің өзінде өздігінен қол қойылған сертификатты қолдансаңыз, оны орнатушының стандартты процедурасын қолдана отырып, Kaspersky Security Center Web Console жаңарту арқылы қайта шығаруға болады (**Жаңарту** параметрі).

Web Console ашқан кезде, браузер сізге Web Console қосылымы жеке емес екенін және Web Console сертификаты жарамсыз екенін хабарлауы мүмкін. Бұл ескерту, Kaspersky Security Center Web Console сертификаты өздігінен қол қоятындықтан және оны Kaspersky Security Center автоматты түрде жасайтындықтан пайда болады. Бұл ескертуді жою немесе болдырмау үшін келесі әрекеттердің бірін орындауға болады:

- Пайдаланушы сертификатын қайта шығарылған кезде көрсетіңіз (ұсынылған нұсқа). Сіздің инфрақұрылымыңызда сенімді болып табылатын және пайдаланушы сертификаттарының талаптарына сәйкес келетін сертификат жасау.
- Сертификатты қайта шығарғаннан кейін, сенімді браузер сертификаттарының тізіміне Web Console сертификатын қосыңыз. Бұл параметрді пайдаланушы сертификатын жасай алмаған жағдайда ғана пайдалану ұсынылады.

Kaspersky Security Center Web Console веб-консолін алғаш орнатқан кезде жаңа сертификат шығару үшін:

1. Kaspersky Security Center Web Console орнатуды іске қосыңыз.
2. Орнату шеберінің **Клиенттік сертификат** қадамына жеткен кезде, **Жаңа сертификатты құру** опциясын таңдап, **Келесі** түймесін басыңыз.
3. Орнату аяқталмайынша, орнату шеберінің барлық қадамдарын орындаңыз.

   Kaspersky Security Center Web Console үшін жаңа сертификат 397 күндік жарамдылық мерзімімен шығарылған.

Мерзімі өткен Kaspersky Security Center Web Console сертификатын қайта шығару үшін:

1. ksc-web-console-<нұсқа_нөмірі>.<жинақ нөмірі>.exe орындалатын файлын әкімші құқықтары бар есептік жазбамен іске қосыңыз.

2. Орнату шеберінің ашылған терезесінде тілді таңдап, **OK** түймесін басыңыз.

3. Сәлемдесу терезесінде **Сертификатты қайта шығару** параметрін таңдап, **Келесі** түймесін басыңыз.

4. Келесі қадамда Kaspersky Security Center Web Console қайта конфигурациялануының аяқталуын күтіп, **Аяқтау** түймесін басыңыз.

   Kaspersky Security Center Web Console сертификаты 397 күндік жарамдылық мерзімімен қайта шығарылған.

Есептік деректер және қатынасу диспетчері қолданылса, Есептік деректер және қатынасу диспетчері қолданылатын порттар үшін барлық TLS сертификаттарын да қайта шығару керек. Kaspersky Security Center Web Console серверінде сертификаттың жарамдылық мерзімі туралы хабарландыру көрсетіледі. Хабарландырудағы нұсқауларды орындаңыз.

Kaspersky Security Center Web Console үшін сертификатты ауыстыру

Әдепкі бойынша, Kaspersky Security Center Web Console серверін орнату кезінде бағдарламаға арналған браузер сертификаты автоматты түрде жасалады. Сіз автоматты түрде жасалған сертификатты пайдаланушы сертификатымен ауыстыра аласыз.

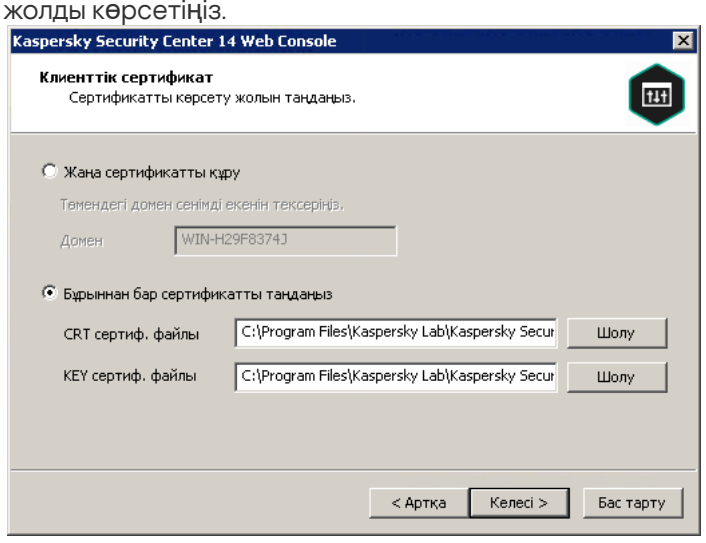
Kaspersky Security Center Web Console сервері үшін сертификатты пайдаланушы сертификатына ауыстыру үшін:

1. Kaspersky Security Center Web Console сервері орнатылған құрылғыда ksc-web-console-<нұсқа нөмірі>.<жинақ нөмірі>.exe орындалатын файлын әкімші құқықтары бар есептік жазбамен іске қосыңыз.

   Орнату шебері іске қосылады.

2. Шебердің бірінші бетінде **Жаңарту** параметрін таңдаңыз.

3. **Клиенттік сертификат** бетінде **Бұрыннан бар сертификатты таңдаңыз** параметрін таңдап, пайдаланушы сертификатына апаратын жолды көрсетіңіз.



Клиенттік сертификатты белгілеу

4. Шебердің соңғы бетінде жаңа параметрлерді қолдану үшін **Өзгерту** түймесін басыңыз.

5. Бағдарламаны орнату сәтті аяқталғаннан кейін **Дайын** түймесін басыңыз.

Kaspersky Security Center Web Console сервері көрсетілген сертификатпен жұмыс істейді.

Сенімді Басқару серверлері үшін сертификаттарды Kaspersky Security Center Web Console веб-консолінде көрсету

Қолданыстағы Басқару сервері сертификаты сертификаттың жарамдылық мерзімі аяқталғанға дейін автоматты түрде жаңасымен ауыстырылады. Сондай-ақ, қолданыстағы Басқару сервері сертификатын пайдаланушы сертификатымен ауыстыруға болады. Сертификат өзгерген сайын, жаңа сертификат Kaspersky Security Center Web Console бағдарламасының параметрлерінде көрсетілуі тиіс. Әйтпесе, Kaspersky Security Center Web Console Басқару серверіне қосыла алмайды.

Басқару серверіне жаңа сертификат орнату үшін:

1. Басқару сервері орнатылған құрылғыда сертификат файлын, мысалы, жаппай сақтау құрылғысына көшіріңіз.

   Әдепкі бойынша сертификат файлы келесі қалтада сақталады:

   - Windows операциялық жүйесі бар құрылғылар үшін: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
   - Linux операциялық жүйесі бар құрылғылар үшін: /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыда сертификат файлын жергілікті қалтаға салыңыз.

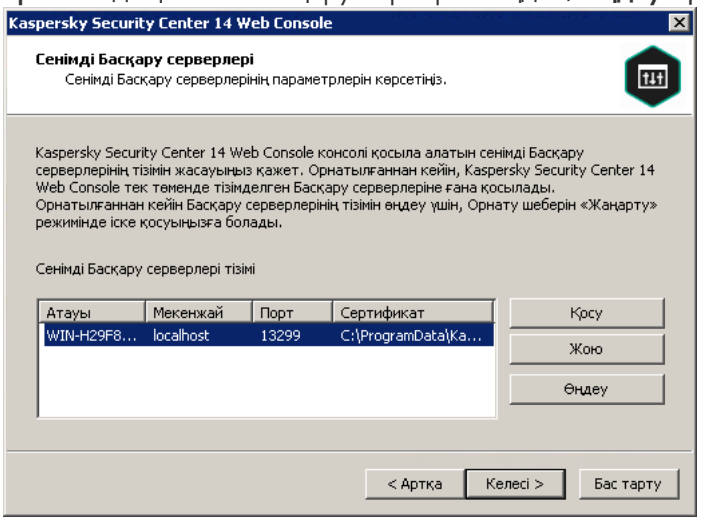
3. ksc-web-console-<нұсқа_нөмірі>.<нұсқа нөмірі>.exe орнату файлын әкімші құқықтары бар есептік жазбамен іске қосыңыз.

   Орнату шебері іске қосылады.

4. Шебердің бетінде **Жаңарту** параметрін таңдаңыз.

   Содан кейін, шебердің нұсқауларын орындаңыз.

5. **Сенімді Басқару серверлері** бетінде қажетті Басқару серверін таңдап, **Өңдеу** түймесін басыңыз.



Сенімді Басқару серверлерін белгілеу

6. Ашылған **Басқару серверін өңдеу** терезесінде **Шолу** түймесін басыңыз, жаңа сертификат файлына апаратын жолды көрсетіңіз және өзгерістерді қолдану үшін **Жаңарту** түймесін басыңыз.

7. Шебердің **Kaspersky Security Center Web Console консолін өзгертуге дайын** бетінде, жаңартуды бастау үшін **Жаңарту** түймесін басыңыз.

8. Бағдарламаны орнату сәтті аяқталғаннан кейін **Аяқтау** түймесін басыңыз.

9. Kaspersky Security Center Web Console веб-консоліне Кіріңіз.

Kaspersky Security Center Web Console сервері көрсетілген сертификатпен жұмыс істейді.

Сертификатты PFX пішімінен PEM пішіміне түрлендіру

Kaspersky Security Center Web Console бағдарламасында PFX пішіміндегі сертификатты пайдалану үшін, оны кез келген OpenSSL негізіндегі кроссплатформалық утилита арқылы PEM пішіміне алдын ала түрлендіру қажет.

Windows операциялық жүйесінде сертификатты PFX пішімінен PEM пішіміне түрлендіру үшін:

1. OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрмендерді орындаңыз:

   ```
   openssl pkcs12 -in <файл атауы.pfx> -clcerts -nokeys -out server.crt
   ```

   ```
   openssl pkcs12 -in <файл атауы.pfx> -nocerts -nodes -out key.pem
   ```

   Нәтижесінде, сіз .crt файлы ретінде жалпыға ортақ кілтті және құпиясөзбен қорғалған .pem файлы ретінде жеке кілтті аласыз.

2. .crt және .pem файлдары .pfx файлы сақталатын қалтада жасалғанына көз жеткізіңіз.

3. Егер .crt немесе .pem файлында "атрибуттар пакеті" бар болса, бұл атрибуттарды кез келген ыңғайлы мәтіндік редактор арқылы жойып, файлды сақтаңыз.

4. Windows қызметін қайта іске қосыңыз.

5. Kaspersky Security Center Web Console сервері құпиясөз тіркесімен қорғалған сертификаттарды қолдамайды. Сондықтан, .pem файлынан құпиясөз тіркесін жою үшін OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрменді орындаңыз:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > .PEM кіріс және шығыс файлдары үшін бірдей атты қолданбаңыз.

   Нәтижесінде, жаңа .pem файлы шифрланбаған. Оны пайдалану үшін құпиясөз тіркесін енгізудің қажеті жоқ.

.crt және .pem файлдары пайдалануға дайын, сондықтан оларды Kaspersky Security Center Web Console орнату шеберінде көрсетуге болады.

Linux операциялық жүйесінде сертификатты PFX пішімінен PEM пішіміне түрлендіру үшін:

1. OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрмендерді орындаңыз:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <файл атауы.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Сертификат файлы мен жеке кілт PFX файлы сақталатын қалтада жасалғанына көз жеткізіңіз.

3. Kaspersky Security Center Web Console сервері құпиясөз тіркесімен қорғалған сертификаттарды қолдамайды. Сондықтан, .pem файлынан құпиясөз тіркесін жою үшін OpenSSL негізіндегі кроссплатформалық утилитада келесі пәрменді орындаңыз:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > .PEM кіріс және шығыс файлдары үшін бірдей атты қолданбаңыз.

   Нәтижесінде, жаңа .pem файлы шифрланбаған. Оны пайдалану үшін құпиясөз тіркесін енгізудің қажеті жоқ.

.crt және .pem файлдары пайдалануға дайын, сондықтан оларды Kaspersky Security Center Web Console орнату шеберінде көрсетуге болады.

Kaspersky Security Center Windows жүйесінен деректерді тасымалдау

Бұл бөлімде басқарылатын құрылғылар мен олармен байланысты нысандардың (саясат, тапсырмалар, топтар, тегтер және басқа нысандар) деректерін Kaspersky Security Center Windows жүйесінен тасымалдау сипатталған.

- Kaspersky Next Expert View
- Kaspersky Security Center Linux

Kaspersky Next Expert View-ге көшу

Сіз деректерді Kaspersky Security Center Web Console веб-консолінен Kaspersky Next Expert View консоліне жылжытуды қолмен орындай аласыз. Осыдан кейін, сіз Kaspersky инфрақұрылымында орналасқан Басқару серверіне және дерекқорларды басқару жүйесіне (ДҚБЖ) қатынаса аласыз. Сізге физикалық сервер немесе ДҚБЖ қажет емес: екеуіне де Kaspersky мамандары қызмет көрсетеді.

Сіз Windows, Linux немесе macOS операциялық жүйелері басқаратын құрылғылардың деректерін Kaspersky Next Expert View басқаруына жібере аласыз. Егер сіздің желіңізде Басқару сервері иерархиясы болса, оны Kaspersky Next Expert View сақтауға болады. Бұдан бөлек, сіз келесіні жылжыта аласыз:

- Басқарылатын бағдарламалардың тапсырмалары мен саясаттары
- Глобалдық тапсырмалар
- Пайдаланушылық құрылғы таңдаулары
- Басқару топтары құрылымы және оған кіретін құрылғылар
- Деректер жылжытылатын құрылғыларға тағайындалған тегтер

Деректерді жылжыту аяқталғаннан кейін, сіз құрылғыларды Kaspersky Next Expert View арқылы басқара аласыз. Бұл ретте, тасымалданатын нысандар сақталады, ал Желілік агент барлық басқарылатын құрылғыларға қайта орнатылады.

Деректерді тасымалдау әдісі және алғышарттар тізімі *Kaspersky Next Expert View анықтамасында* көрсетілген.

Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы-ке көшіру

Осы сценарий арқылы басқару тобының құрылымын, сонымен қатар басқарылатын құрылғыларды және топтың басқа нысандарын (саясаттарды, тапсырмаларды, жаһандық тапсырмаларды, тегтерді және құрылғы таңдауларын) Kaspersky Security Center Windows жүйесінен Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқаруына тасымалдауға болады.

Шектеулер:

- Деректерді тек Kaspersky Security Center 14.2 Windows жүйесінен Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы 1.0 нұсқасынан бастап тасымалдауға болады.
- Бұл сценарийді тек Kaspersky Security Center Web Console көмегімен орындауға болады.

Кезеңдер

Деректерді тасымалдау сценарийі келесі қадамдардан тұрады:

1. **Деректерді тасымалдау әдісін таңдаңыз**

   Деректерді Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы серверіне тасымалдау шеберімен тасымалдау керек. Тасымалдау шеберінің қадамдары Kaspersky Security Center Windows және Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқару серверлері иерархияға реттелгеніне байланысты:

   - Басқару серверлерінің иерархиясы арқылы деректерді тасымалдау

     Kaspersky Security Center Windows басқару сервері Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқару серверіне бағынышты болса, осы опцияны таңдаңыз. Сіз деректерді тасымалдау процесін басқарасыз және OSMP Console веб-консолінің бір үлгісі шеңберінде Серверлер арасында ауысасыз. Бұл нұсқаны артық көрсеңіз, деректерді тасымалдау рәсімін жеңілдету үшін Басқару серверлерін иерархия түрінде ұйымдастыра аласыз. Мұны істеу үшін деректерді тасымалдауды бастамас бұрын иерархияны жасаңыз.

   - Деректерді экспорттау файлы (ZIP мұрағаты) арқылы тасымалдау

     Kaspersky Security Center Windows және Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқару серверлері иерархияда орналаспаған болса, осы опцияны таңдаңыз. Деректерді тасымалдау процесін екі консоль көмегімен басқарасыз: Kaspersky Security Center Windows және Kaspersky Security Center Console. Бұл жағдайда сіз Kaspersky Security Center Windows жүйесінен экспорттау кезінде жасаған және жүктеп алған экспорттау файлын пайдаланасыз және бұл файлды Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы жүйесіне импорттайсыз.

2. **Kaspersky Security Center Windows жүйесінен деректерді экспорттау**

   Kaspersky Security Center Windows жүйесін ашып, деректерді тасымалдау шеберін іске қосыңыз.

3. **Деректерді Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы бағдарламасына импорттау**

   Экспортталған деректерді Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы жүйесіне импорттау үшін тасымалдау шеберімен жұмыс істеуді жалғастырыңыз.

   Серверлер иерархияға ұйымдастырылған болса, импорттау сол шеберде сәтті экспорттаудан кейін автоматты түрде басталады. Серверлер иерархияда орналаспаса, Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы жүйесіне ауысқаннан кейін, тасымалдау шеберімен жұмыс істеуді жалғастырасыз.

4. **Kaspersky Security Center Windows жүйесінен Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы жүйесіне нысандар мен параметрлерді қолмен тасымалдау үшін қосымша қадамдарды орындау (қосымша қадам)**

   Сондай-ақ деректерді тасымалдау шебері арқылы тасымалдау мүмкін емес нысандар мен параметрлерді тасымалдауға болады. Мысалы, қосымша келесі әрекеттерді орындауға болады:

   - Басқару серверінің жаһандық тапсырмаларын конфигурациялау
   - Желілік агент саясаты параметрлерін конфигурациялау
   - Бағдарламаларды орнату пакеттерін жасау
   - Виртуалды басқару серверлерін жасау
   - Тарату нүктелерін тағайындау және конфигурациялау
   - Құрылғыларды жылжыту ережелерін конфигурациялау
   - Құрылғыларға автоматты түрде тег қою ережелерін конфигурациялау
   - Бағдарламалар санаттарын жасау

5. **Импортталған басқарылатын құрылғыларды Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқаруына жылжыту**

   Көшіруді аяқтау үшін Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқаруындағы импортталған басқарылатын құрылғыларды жылжытыңыз. Келесі әдістердің бірін пайдалана аласыз:

   - Kaspersky Security Center топтық тапсырмасы арқылы

     Белгілі бір клиенттік құрылғылар үшін басқару серверін басқасына өзгерту үшін Басқару серверін өзгерту тапсырмасын пайдаланыңыз.

   - klmover утилитасын пайдалану арқылы

     klmover утилитасын пайдаланыңыз және жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз.

   - Басқарылатын құрылғыларда желілік агентті орнату немесе қайта орнату арқылы.

     Желілік агентті орнату пакетін жасаңыз және орнату пакетінің сипаттарында жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз. Орнату пакетін пайдаланып, қашықтан орнату тапсырмасы арқылы импортталған басқарылатын құрылғыларға желілік агентті орнатыңыз.

     Сондай-ақ желілік агентті жергілікті түрде орнату үшін автономды орнату бумасын жасауға және пайдалануға болады.

6. **Желілік агентті соңғы нұсқаға жаңартыңыз**

   Желілік агентті Kaspersky Security Center Console нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

7. **Басқарылатын құрылғылардың жаңа басқару серверінде көрінетініне көз жеткізіңіз**

   Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы басқару серверінде басқарылатын құрылғылар тізімін ашыңыз (**Активтер (құрылғылар)** → **Басқарылатын құрылғылар**) және **Көзге көрінетін**, **Желілік агент орнатылған** және **Басқару серверіне соңғы қосылу уақыты** бағандарындағы мәндерді тексеріңіз.

Деректерді тасымалдаудың басқа әдістері

Деректерді тасымалдау шеберінен басқа, нақты бір тапсырмалар мен саясаттарды да тасымалдауға болады:

- Тапсырмаларды Kaspersky Security Center Windows жүйесінен экспорттаңыз, содан кейін Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы жүйесіне импорттаңыз.
- Саясаттарды Kaspersky Security Center Windows жүйесінен экспорттаңыз, содан кейін Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы жүйесіне импорттаңыз. Байланыстырылған саясат профильдері таңдалған саясаттармен бірге экспортталады және импортталады.

Kaspersky Security Center Linux бағдарламасына тасымалдау

Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне көшіру Басқару сервері деректерінің сақтық көшірмесін (klbackup utility утилитасымен) және Тасымалдау шеберін пайдалану арқылы қолжетімді.

Төмендегі кесте басқару сервері деректерінің сақтық көшірмесін және тасымалдау шеберін пайдалану арқылы көшірудің негізгі мүмкіндіктері мен шектеулерін салыстыруға, қай тәсіл ұйымыңыз үшін қолайлы екенін шешуге мүмкіндік береді.

Параметрлер	Басқару сервері деректерін сақтық көшірмелеу	Тасымалдау шебері
Көшіру процесі	Kaspersky Security Center Windows басқару сервері деректерінің толық сақтық көшірмесін жасау және оны Kaspersky Security Center Linux басқару серверінде қалпына келтіру	Көшіру үшін басқару сервері деректерін таңдау және экспорттау, бұл деректерді Kaspersky Security Center Linux басқару серверіне импорттау және Kaspersky Security Center Linux басқаратын құрылғыларды ауыстыру
Көшіру әдісінің мүмкіндіктері	• Барлық басқару сервері дерегін көшіру • Басқарылатын құрылғылардың кез келген санын көшіру • Kaspersky Security Center Windows басқару сервері деректерінің толық көшірмесін алу және оны Kaspersky Security Center Linux басқару серверіне тасымалдау үшін пайдаланылады	• Басқару сервері деректерін ішінара көшіру • Көшіру үшін нысандарды таңдау қолжетімді • Көшірілетін басқару тобы немесе ішкі топ 10000 құрылғыдан аспауы керек • Басқару сервері деректерін, соның ішінде тек көшіру ауқымындағы топтық нысандарды ішінара тасымалдау үшін пайдаланылады; көшіру ауқымынан тыс топтық нысандар қолмен қалпына келтірілуі керек
Көшіру ауқымы	Басқарылатын құрылғылардың шектеусіз санымен басқару сервері деректерін толық тасымалдау	• Басқару тобының құрылымы • Басқару топтарына қосылған басқарылатын құрылғылар (**10000 құрылғыдан аспайды**) • Көшіру құрылғыларына тағайындалған тегтер • Желілік агенттің жаһандық тапсырмалары және басқарылатын қолданбалар (басқару серверіне арналмаған) • Желілік агент пен басқарылатын қолданбалардың топтық тапсырмалары • Басқарылатын қолданбалардың саясаттары • Есеп үлгілері • Пайдаланушы рөлдері • Ішкі пайдаланушылар және қауіпсіздік топтары • Қолмен қосылған мазмұны бар арнаулы қолданба санаттары • Пайдаланушылық құрылғы таңдаулары
Көшірілмеген ауқым	—	• Басқару серверінің жаһандық тапсырмалары • Басқару серверінде сақталған оқиғалар • Қашықтан орнатуға арналған қолданбалар дистрибутивтерінің қоймасы • Басқару сервері сертификаты • Басқару сервері және басқарылатын қолданбалар пайдаланатын лицензия кілттері • Виртуалды Басқару серверлері • Желілік агент саясатының параметрлері • Құрылғыны жылжыту ережелері • Құрылғыларға автоматты түрде тэг енгізу ережелері • Тарату нүктелері • Басқару серверінде сақталған Kaspersky қолданба параметрлері
Көшіруді қолдайтын Kaspersky Security Center нұсқалары	• Kaspersky Security Center Windows жүйесінің кез келген қолдау көрсетілетін нұсқасы • Kaspersky Security Center Linux 15.2 немесе одан кейінгі нұсқасы	• Kaspersky Security Center Windows 14.2 немесе одан кейінгі нұсқасы • Kaspersky Security Center Linux 15 немесе одан кейінгі нұсқасы
Көшіруге болатын ДҚБЖ-лар	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (тек Kaspersky Security Center Windows 14.2 немесе одан кейінгі нұсқасынан орнатылған патчпен Kaspersky Security Center Linux 15.3 немесе одан кейінгі нұсқасына көшіру) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (тек Kaspersky Security Center Windows 15.1 немесе одан кейінгі нұсқасынан Kaspersky Security Center Linux 16 немесе одан кейінгі нұсқасына көшіру үшін)	Қолдау көрсетілетін ДҚБЖ-лар арасында шектеусіз көшіру

Басқару сервері деректерінің сақтық көшірмесін жасау арқылы Kaspersky Security Center Linux жүйесіне тасымалдау

Kaspersky Security Center Linux-ке Kaspersky Security Center Windows басқару серверінің деректерін жылжыту үшін деректердің сақтық көшірмесін пайдалануға болады. Тасымалдау алдында Kaspersky Security Center Windows жүйесінің қажетті мүмкіндіктеріне Kaspersky Security Center Linux жүйесінде қолдау көрсетілетініне көз жеткізіңіз.

Шектеулер:

- Келесі ДҚБЖ-лар арасында тасымалдауға болады:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Microsoft SQL Server, MySQL немесе MariaDB дерекқорында сақталған басқару сервері деректерін MySQL немесе MariaDB жүйесіне көшіруге Kaspersky Security Center Windows жүйесінің кез келген қолдау көрсетілетін нұсқасынан Kaspersky Security Center Linux 15.2 немесе одан кейінгі нұсқасына тасымалдауға қолдау көрсетіледі.
- PostgreSQL дерекқорында сақталған басқару сервері деректерін PostgreSQL жүйесіне немесе Postgres Pro деректерін Postgres Pro жүйесіне көшіруге Kaspersky Security Center Windows 15.1 немесе одан кейінгі нұсқасынан Kaspersky Security Center Linux 16 немесе одан кейінгі нұсқасына көшіруге қолдау көрсетіледі.
- Microsoft SQL Server дерекқорында сақталған басқару сервері деректерін PostgreSQL немесе Postgres Pro жүйесіне көшіруге Kaspersky Security Center Windows 14.2 немесе одан кейінгі нұсқасынан Kaspersky Security Center Linux 15.3 немесе одан кейінгі нұсқасына көшіруге қолдау көрсетіледі.

  PostgreSQL немесе Postgres Pro жүйесіне көшіруге қолдау көрсету үшін келесі әрекеттердің бірін орындауға болады:

  - Kaspersky Security Center Windows басқару сервері үшін 15.1.0.20748-pf2 патчын орнатыңыз. Бұл патчты алу үшін Kaspersky техникалық қолдау қызметіне хабарласыңыз.
  - Kaspersky Security Center Windows жүйесін 15.1.0.22239 нұсқасына жаңартыңыз.
- Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін ДҚБЖ ретінде MySQL немесе MariaDB жүйесін пайдалансаңыз, `lower_case_table_names` параметрі ағымдағы және жаңа ДҚБЖ үшін сәйкес келуі керек.

  Деректердің сақтық көшірмесін жасамай тұрып, `lower_case_table_names` параметрін тексеріңіз. Содан кейін Kaspersky Security Center Linux үшін MySQL немесе MariaDB орнатқан кезде, бұл параметрді Windows жүйесіне арналған осы параметр үшін көрсетілген мәнге орнатуыңыз керек.

Кезеңдер

Басқару сервері деректерінің сақтық көшірмесін пайдалану арқылы тасымалдау кезең-кезеңімен жүзеге асырылады:

1. **Басқару серверіне кіруге болатын әкімшінің ішкі пайдаланушы есептік жазбасы бар екенін тексеру**

   Әкімшінің есептік жазбасы Kaspersky Security Center Linux басқару серверіне кіру үшін пайдаланылады. Сізде бұл есептік жазба болмаса және тек жергілікті Windows есептік жазбасымен немесе домен есептік жазбасымен кірсеңіз, сақтық көшірмені қалпына келтіргеннен кейін Kaspersky Security Center Linux басқару серверіне кіре алмайсыз. Kaspersky Security Center Linux басқару сервері жергілікті Windows есептік жазбасын пайдалану арқылы жүйеге кіруге қолдау көрсетпейді. Домен есептік жазбасы арқылы кіруге болады, бірақ ол үшін басқару серверінің қосымша конфигурациясы қажет болуы мүмкін.

   Сізде әкімшінің есептік жазбасы болмаса, kladduser утилитасын пайдалану арқылы сақтық көшірмені қалпына келтіргеннен кейін осы есептік жазбаны жасау керек болады.

2. **Kaspersky Security Center Windows басқару сервері деректерінің жаңартылған сақтық көшірмесін жасау**

   Kaspersky Security Center Windows және Kaspersky Security Center Linux үшін пайдаланылатын ДҚБЖ түріне байланысты келесі әрекеттердің бірін орындаңыз:

   - MySQL немесе MariaDB жүйесін MySQL немесе MariaDB жүйесіне көшіру үшін: klbackup утилитасын немесе басқару сервері орнатылған құрылғыдағы деректердің сақтық көшірмесін жасау тапсырмасын пайдалану арқылы сақтық көшірме жасаңыз.

   - PostgreSQL-ден PostgreSQL-ге және Postgres Pro-дан Postgres Pro-ға: klbackup утилитасын пайдалану арқылы сақтық көшірме немесе Басқару сервері орнатылған құрылғыда деректердің сақтық көшірмесін жасау тапсырмасын жасаңыз.

   - Microsoft SQL серверін MySQL немесе MariaDB жүйесіне көшіру үшін: klbackup утилитасын қолданып, **MySQL/MariaDB пішіміне көшіру** опциясы қосылған күйде сақтық көшірме жасаңыз.

   - Microsoft SQL серверін PostgreSQL немесе Postgres Pro жүйесіне көшіру үшін:

     1. Kaspersky техникалық қолдау қызметінен сұрап, PostgreSQL және Postgres Pro жүйесіне көшіруге қолдау көрсету үшін басқару серверіне арналған 15.1.0.20748-pf2 патчын орнатыңыз.

        Болмаса Kaspersky Security Center Windows жүйесін 15.1.0.22239 нұсқасына жаңартуға болады.

     2. klbackup утилитасын пайдалану арқылы сақтық көшірме жасаңыз.

        Егер пәрмен жолынан klbackup іске қоссаңыз, `-migrate postgres` жалаушасын пайдаланыңыз.

        Klbackup интерфейсін пайдалансаңыз, **Postgres форматына көшіру** опциясын қосыңыз.

   Сақтық көшірмені жасағаннан кейін Kaspersky Security Center Windows басқару серверін желіден ажыратыңыз.

3. **Kaspersky Security Center Linux орнату үшін жаңа құрылғыны дайындау**

Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

1. Басқару сервері орнатылатын жаңа құрылғыны таңдаңыз. Бұл құрылғы аппараттық және бағдарламалық жасақтама талаптарына сай болуы керек. Басқару серверінде қолданылатын порттардың қолжетімді екеніне көз жеткізіңіз.

2. Жаңа құрылғыға сол мекенжайды тағайындаңыз.

   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk қызметтік бағдарламасын қолданып, басқарылатын құрылғыларда алуға болады).

4 ДҚБЖ орнату және конфигурациялау

Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

1. Оңтайлы өнімділікті қамтамасыз ететін ДҚБЖ түрін таңдаңыз. Желіге қосылған құрылғылардың санын, желі топологиясын және желідегі жұмыс жүктемесін ескеріңіз. Сіз ДҚБЖ қолданатын платформалардың бірін таңдай аласыз.

2. Сақтық көшірме жасау кезінде таңдалған ДҚБЖ түріне сәйкес ДҚБЖ орнатыңыз. Таңдалған ДҚБЖ жүйесін қалай орнату керектігі туралы мәліметтер оның құжаттамасында келтірілген.

   > Дерекқордың жаңа нұсқасы ағымдағы нұсқадан төмен болмауы керек.

3. Kaspersky Security Center Linux-пен жұмыс істеу үшін ДҚБЖ-ны конфигурациялаңыз.

5 Kaspersky Security Center Linux орнату

Kaspersky Security Center Linux жүйесін жаңа құрылғыға орнатыңыз.

Орнату кезінде жасалған әкімшінің ішкі пайдаланушы есептік жазбасы, сондай-ақ сақтық көшірмеден басқару серверінің деректерін қалпына келтірмей тұрып жасалған басқа нысандар (топтар, саясаттар, тапсырмалар, пайдаланушылар) қалпына келтіргеннен кейін жоғалады. Бұл нысандар сақтық көшірмеде қамтылған нысандармен ауыстырылады.

6 Сақтық көшірмеден басқару сервер деректерін қалпына келтіру

Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

1. klbackup утилитасын пайдалану арқылы жаңа құрылғыда басқару сервері деректерін қалпына келтіріңіз.

2. Сізде Kaspersky Security Center Windows басқару серверіне кірген әкімшінің ішкі пайдаланушы есептік жазбасы болмаса және жергілікті Windows есептік жазбасын немесе домен есептік жазбасын пайдаланасаңыз, kladduser утилитасын пайдаланып, әкімші есептік жазбасын келесідей жасаңыз:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   мұндағы `<password>` параметрі келесі талаптарға сәйкес келеді:

   - Пайдаланушының құпиясөзі 8 таңбадан кем немесе 256 таңбадан аспауы керек.
   - Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
     - Бас әріптер (A-Z)
     - Кіші әріптер (a-z)

- Сандар (0-9)
- Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Kaspersky Security Center Web Console орнату және басқару серверін конфигурациялау**

   Сценарийдің осы қадамында келесі әрекеттерді орындаңыз:

   1. Kaspersky Security Center Web Console веб-консолін орнатыңыз.

      Kaspersky Security Center Web Console бұрын орнатылған болса, оны сол жауап файлымен қайта орнатыңыз.

      Әкімшінің ішкі пайдаланушы есептік жазбасы арқылы Kaspersky Security Center Web Console-ге кіріңіз.

      Деректерді жұмысқа дайындау процесі басқару серверінің деректерін қалпына келтіргеннен кейін әдетте 15 минутқа дейін созылады, бірақ уақыт аппараттық жасақтама өнімділігіне және басқару сервері деректерінің өлшеміне байланысты. Осы уақыт ішінде Kaspersky Security Center Web Console қосылмауы және қателерді көрсетуі мүмкін.

   2. Дерекқордағы деректерді жұмысқа дайындау аяқталған кезде, басқару серверінің негізгі мүмкіндіктерінің жұмыс істейтінін тексеріңіз. Басқару сервері басқарылатын құрылғылармен синхрондалатынын және басқару сервері деректерінің қалпына келтірілгенін тексеріңіз.

   3. Домен құрылымы, пайдаланушы есептік жазбалары, қауіпсіздік топтары және домендерге қосылған құрылғылардың DNS атаулары туралы ақпаратты қалпына келтіру үшін домен контроллерлеріне сауалнама жүргізіңіз.

   4. Қажет болса, алдыңғы құрылғыдан басқару сервері мен дерекқор серверін жойыңыз.

      Бір желіде қосылым мекенжайы мен басқару серверінің сертификаты бірдей бірнеше басқару сервері болмауы керек.

Әкімші Kaspersky Security Center Linux жүйесінде қолдау көрсетілетін функцияларды ескере отырып, Kaspersky Security Center Windows жүйесінде болған басқарылатын құрылғыларға және басқару серверінің деректеріне қол жеткізе алады.

Kaspersky Security Center Linux серверіне тасымалдау шеберімен тасымалдау

Осы сценарий арқылы басқару тобының құрылымын, сонымен қатар басқарылатын құрылғыларды және топтың басқа нысандарын (саясаттарды, тапсырмаларды, жаһандық тапсырмаларды, тегтерді және құрылғы таңдауларын) Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux басқаруына тасымалдауға болады. Тасымалдау алдында Kaspersky Security Center Windows жүйесінің қажетті мүмкіндіктеріне Kaspersky Security Center Linux жүйесінде қолдау көрсетілетініне көз жеткізіңіз.

Шектеулер:

- Деректерді тек Kaspersky Security Center Windows 14.2 және одан жоғары нұсқасынан Kaspersky Security Center Linux 15 және одан жоғары нұсқасына тасымалдауға болады.
- Бұл сценарийді тек Kaspersky Security Center Web Console көмегімен орындауға болады.

Кезеңдер

Деректерді тасымалдау сценарийі келесі қадамдардан тұрады:

1. **Деректерді тасымалдау әдісін таңдаңыз**

   Деректерді Kaspersky Security Center Linux серверіне деректерді тасымалдау шеберімен тасымалдап жатырсыз. Деректерді тасымалдау шеберінің әрекеттері Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияға реттелгеніне байланысты:

   - Басқару серверлерінің иерархиясы арқылы деректерді тасымалдау

     Kaspersky Security Center Windows Басқару сервері Kaspersky Security Center Linux Басқару серверіне бағынышты болса, осы параметрді таңдаңыз. Сіз деректерді тасымалдау процесін басқарасыз және Kaspersky Security Center Web Console веб-консолінің бір үлгісі шеңберінде Серверлер арасында ауысасыз. Бұл нұсқаны артық көрсеңіз, деректерді тасымалдау рәсімін жеңілдету үшін Басқару серверлерін иерархия түрінде ұйымдастыра аласыз. Мұны істеу үшін деректерді тасымалдауды бастамас бұрын иерархияны жасаңыз.

   - Деректерді экспорттау файлы (ZIP мұрағаты) арқылы тасымалдау

     Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияда реттелмеген болса, осы параметрді таңдаңыз. Сіз деректерді тасымалдау процесін Kaspersky Security Center Web Console екі данасын, Kaspersky Security Center Windows жүйесінің бір данасын және Kaspersky Security Center Linux басқа данасын пайдалану арқылы басқарасыз. Бұл жағдайда сіз Kaspersky Security Center Windows жүйесінен экспорттау кезінде жасаған және жүктеп алған экспорттау файлын пайдаланасыз және бұл файлды Kaspersky Security Center Linux жүйесіне импорттайсыз.

2. **Kaspersky Security Center Windows Басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасау (қосымша қадам)**

   Сақтық көшірмеден Басқару серверінің сертификаты мен жеке кілтін қалпына келтіру арқылы басқарылатын құрылғыларды Kaspersky Security Center Linux Басқару серверінің басқаруына орналастырғыңыз келуі мүмкін. Бұл жағдайда Kaspersky Security Center Windows басқару серверінің сертификаты мен жеке кілтінің сақтық көшірмесін жасаңыз. Содан кейін 6-қадамда сертификат пен жеке кілтті қалпына келтіріңіз.

3. **Kaspersky Security Center Windows жүйесінен деректерді экспорттау**

   Kaspersky Security Center Windows жүйесін ашып, деректерді тасымалдау шеберін іске қосыңыз.

4. **Деректерді Kaspersky Security Center Linux бағдарламасына импорттау**

   Экспортталған деректерді Kaspersky Security Center Linux жүйесіне импорттау үшін деректерді тасымалдау шеберімен жұмыс істеуді жалғастырыңыз. Серверлер иерархияға ұйымдастырылған болса, импорттау сол шеберде сәтті экспорттаудан кейін автоматты түрде басталады. Серверлер иерархияда орналаспаса, Kaspersky Security Center Linux жүйесіне ауысқаннан кейін, деректерді тасымалдау шеберімен жұмыс істеуді жалғастырасыз.

5. **Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне нысандар мен параметрлерді қолмен тасымалдау үшін қосымша қадамдарды орындау (қосымша қадам)**

   Сондай-ақ деректерді тасымалдау шебері арқылы тасымалдау мүмкін емес нысандар мен параметрлерді тасымалдауға болады. Мысалы, қосымша келесі әрекеттерді орындауға болады:

   - Басқару сервері және басқарылатын бағдарламалар пайдаланатын лицензия кілттерін тасымалдаңыз
   - Басқару серверінің жаһандық тапсырмаларын конфигурациялау
   - Желілік агент саясаты параметрлерін конфигурациялау

- Бағдарламаларды орнату пакеттерін жасау
- Виртуалды басқару серверлерін жасау
- Тарату нүктелерін тағайындау және конфигурациялау
- Құрылғыларды жылжыту ережелерін конфигурациялау
- Құрылғыларға автоматты түрде тег қою ережелерін конфигурациялау
- Бағдарламалар санаттарын жасау

6. **Импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына жылжыту**

   Деректерді тасымалдауды аяқтаңыз, импортталған басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруына жылжытыңыз. Келесі әдістердің бірін пайдалана аласыз:

   - klmover утилитасын пайдалану арқылы

     klmover утилитасын пайдаланыңыз және жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз.

   - *Басқару серверін өзгерту* тапсырманың көмегімен

     Басқару серверін өзгерту тапсырмасын жасап, импортталған басқарылатын құрылғыларды, жаңа Басқару серверін және басқа тапсырма параметрлерін көрсетіңіз. Содан кейін басқарылатын құрылғыларды Kaspersky Security Center Linux Басқару серверінің басқаруына орналастыру тапсырмасын орындаңыз.

   - Жою (егер орнатылған болса), содан кейін басқарылатын құрылғыларда Желілік агентін орнату арқылы

     Желілік агентті орнату пакетін жасаңыз және орнату пакетінің сипаттарында жаңа басқару сервері үшін қосылым параметрлерін көрсетіңіз. Импортталған басқарылатын құрылғыларда Network Agent бағдарламасын жойыңыз, содан кейін қашықтан орнату тапсырмасын пайдаланып осы құрылғыларға Желілік агентін орнату үшін орнату бумасын пайдаланыңыз. Сондай-ақ желілік агентті жергілікті түрде орнату үшін автономды орнату бумасын жасауға және пайдалануға болады. Толық ақпаратты Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру бөлімінен қараңыз.

   - Сертификатты және басқару серверінің жеке кілтін сақтық көшірмеден қалпына келтіру арқылы (тек Kaspersky Security Center Linux 15.1 және одан кейінгі нұсқасына тасымалдау үшін)

     Kaspersky Security Center Linux басқару сервері бар құрылғыға Kaspersky Security Center Windows басқару серверінікімен бірдей желі мекенжайын тағайындаңыз. Басқару серверінің сертификаты мен жеке кілтін 2-қадамда сақталған сақтық көшірмеден қалпына келтіру үшін `-cert_only` параметрі бар klbackup утилитасын іске қосыңыз. Пәрмен жолында келесі пәрменді орындаңыз: `/opt/kaspersky/ksc64/sbin/klbackup -path <басқару сервері сертификатының сақтық көшірме жолы> -restore -cert_only`. Қосымша ақпарат алу үшін Басқа басқару серверінің басқаруымен басқарылатын құрылғыларды ауыстыру үшін klbackup утилитасын пайдалану бөлімін қараңыз.

7. **Желілік агентті соңғы нұсқаға жаңартыңыз**

   Linux үшін желілік агентті Kaspersky Security Center нұсқасымен бірдей нұсқаға жаңарту ұсынылады.

8. **Басқарылатын құрылғылардың жаңа басқару серверінде көрінетініне көз жеткізіңіз**

   Kaspersky Security Center Linux Басқару серверінде басқарылатын құрылғылар тізімін ашыңыз (**Активтер (құрылғылар)** → **Басқарылатын құрылғылар**) және **Көзге көрінетін**, **Желілік агент орнатылған** және **Басқару серверіне соңғы қосылу уақыты** бағандарындағы мәндерді тексеріңіз.

Деректерді тасымалдаудың басқа әдістері

Деректерді тасымалдау шеберінен басқа, нақты бір тапсырмалар мен саясаттарды да тасымалдауға болады:

- Тапсырмаларды Kaspersky Security Center Windows жүйесінен экспорттаңыз, содан кейін Kaspersky Security Center Linux жүйесіне импорттаңыз.
- Белгілі бір саясаттарды Kaspersky Security Center Windows жүйесінен экспорттаңыз, содан кейін саясаттарды Kaspersky Security Center Linux жүйесіне импорттаңыз. Байланыстырылған саясат профильдері таңдалған саясаттармен бірге экспортталады және импортталады.

Kaspersky Security Center Windows жүйесінен топтық нысандарды экспорттау

Басқарылатын құрылғыларды және басқа топ нысандарын қамтитын басқару тобының құрылымын Kaspersky Security Center Windows жүйесінен Kaspersky Security Center Linux жүйесіне тасымалдау үшін алдымен экспортталатын деректерді таңдап, экспорттау файлын жасау керек. Экспорттау файлы тасымалдағыңыз келетін барлық топ нысандары туралы ақпаратты қамтиды. Экспорттау файлы Kaspersky Security Center Linux жүйесіне кейіннен импорттау үшін пайдаланылады.

Сіз келесі нысандарды экспорттай аласыз:

- Басқарылатын бағдарламалардың тапсырмалары мен саясаттары
- Глобалдық тапсырмалар
- Пайдаланушылық құрылғы таңдаулары
- Басқару топтары құрылымы және оған кіретін құрылғылар
- Деректер жылжытылатын құрылғыларға тағайындалған тегтер

Экспорттауды бастау алдында Kaspersky Security Center Linux жүйесіне деректерді тасымалдау туралы жалпы ақпаратты оқыңыз. Деректерді тасымалдау тәсілін таңдаңыз: Kaspersky Security Center Windows және Kaspersky Security Center Linux Басқару серверлері иерархиясын пайдаланып немесе пайдаланбай.

Деректерді тасымалдау шебері арқылы басқарылатын құрылғылар мен байланыстырылған топтық нысандарды экспорттау үшін:

1. Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияда реттелгеніне қарай, келесі әрекеттердің бірін орындаңыз:
   - Серверлер иерархияда орналасса, Kaspersky Security Center Web Console веб-консолін ашып, Kaspersky Security Center Windows Басқару серверіне ауысыңыз.
   - Серверлер иерархияда реттелмесе, Kaspersky Security Center Windows жүйесіне қосылған Kaspersky Security Center Web Console веб-консолін ашыңыз.
2. Бағдарламаның негізгі терезесінде **Операциялар** → **Тасымалдау** бөліміне өтіңіз.

3. Шеберді іске қосу және оның қадамдарын орындау үшін деректер мен параметрлерді тасымалдау қажет жерді таңдаңыз.

    - Деректер мен параметрлерді Kaspersky Security Center Cloud Console ішіне тасымалдағыңыз келсе, **Kaspersky Security Center Cloud Console консоліне көшірілді** параметрін таңдаңыз.

    - Деректер мен параметрлерді Kaspersky Security Center Linux немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы ішіне тасымалдағыңыз келсе, **Kaspersky Security Center Linux немесе Open Single Management Platform платформасына көшіру** опциясын таңдаңыз.

4. Экспорттағыңыз келетін басқару тобын немесе ішкі тобын таңдаңыз. Таңдалған басқару тобында немесе ішкі тобында 10 000-нан аспайтын құрылғы болуы керек екенін ескеріңіз.

5. Тапсырмалары мен саясаттары экспортталатын басқарылатын бағдарламаларды таңдаңыз. Тек Kaspersky Security Center Linux қолдайтын бағдарламаларды таңдаңыз. Қолдау көрсетілмейтін бағдарламалардың нысандары әлі де экспортталады, бірақ жұмыс істемейді.

6. Глобалдық тапсырмаларды, құрылғы таңдауларын және экспорттау есептерін таңдау үшін сол жақтағы сілтемелерді пайдаланыңыз. **Топ нысандары** сілтемесі пайдаланушылардың, ішкі пайдаланушылардың және қауіпсіздік топтарының рөлдерін, сондай-ақ бағдарламалардың пайдаланушы санаттарын экспорттаудан алып тастауға мүмкіндік береді.

Экспорттау файлы (ZIP мұрағаты) жасалды. Басқару сервері иерархиясын қолдау арқылы деректерді тасымалдайтыныңызға байланысты экспорттау файлы келесідей сақталады:

- Серверлер иерархияда реттелген болса, экспорттау файлы Kaspersky Security Center Web Console серверіндегі уақытша қалтаға сақталады.

- Серверлер иерархияда ұйымдастырылмаған болса, экспорттау файлы құрылғыңызға жүктеледі.

Басқару сервері иерархиясын қолдау арқылы деректерді тасымалдаған кезде, импорттау сәтті экспорттаудан кейін автоматты түрде басталады. Басқару сервері иерархиясының қолдауынсыз деректерді тасымалдаған кезде, сақталған экспорттау файлын Kaspersky Security Center Linux жүйесіне қолмен импорттауға болады.

Экспорттық файлын Kaspersky Security Center Linux жүйесіне импорттау

Kaspersky Security Center Windows жүйесінен экспорттаған басқарылатын құрылғылар, нысандар және олардың параметрлері туралы ақпаратты тасымалдау үшін оны Kaspersky Security Center Linux немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы қолданбасына импорттау қажет.

Деректерді тасымалдау шебері арқылы басқарылатын құрылғылар мен топтың байланыстырылған нысандарын импорттау үшін:

1. Kaspersky Security Center Windows және Kaspersky Security Center Linux басқару серверлері иерархияда реттелгеніне қарай, келесі әрекеттердің бірін орындаңыз:

   - Серверлер иерархияға реттелген болса, экспорттауды аяқтағаннан кейін деректерді тасымалдау шеберінің келесі қадамына өтіңіз. Бұл шеберде сәтті экспорттаудан кейін импорт автоматты түрде басталады (осы нұсқадың 2-қадамын қараңыз).

   - Серверлер иерархияға реттелмесе:

     a. Kaspersky Security Center Linux немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы қолданбасына қосылған Kaspersky Security Center Web Console ашыңыз.

     b. Бағдарламаның негізгі терезесінде **Операциялар** → **Тасымалдау** бөліміне өтіңіз.

     c. Kaspersky Security Center Windows жүйесінен экспорттау кезінде жасаған және жүктеп алған экспорттау файлын (ZIP мұрағаты) таңдаңыз. Экспорттау файлы жүктеле бастайды.

2. Экспорттау файлы сәтті жүктелгеннен кейін, импорттауды жалғастыра аласыз. Экспортталатын басқа файлды көрсеткіңіз келсе, **Өзгерту** сілтемесін басып, қажетті файлды таңдаңыз.

3. Kaspersky Security Center Linux басқару топтардың бүкіл иерархиясы көрсетіледі.

   Экспортталған басқару топтың нысандарын (басқарылатын құрылғылар, саясаттар, тапсырмалар және басқа топ нысандары) қалпына келтіргіңіз келетін мақсатты басқару топтың жанындағы жалаушаны белгілеңіз.

4. Топтық нысандарды импорттау басталады. Импорттау кезінде деректерді тасымалдау шеберін жия алмайсыз немесе кез келген әрекеттерді бірге орындай алмайсыз. Нысандар тізіміндегі барлық тармақтардың жанындағы белгішелер (🔄) жасыл жалаушаларға (✓) ауысқанын және импорттау аяқталғанын күтіңіз.

5. Импорттау аяқталған кезде, экспортталған басқару топтың құрылымы, соның ішінде құрылғылар туралы ақпарат таңдалған мақсатты басқару топта пайда болады. Қалпына келтірілетін нысанның атауы бар нысанның атымен бірдей болса, қалпына келтірілген нысанға қосымша жұрнақ қосылады.

> Егер кейінге қалдырылған тапсырмада іске қосылатын есептік жазбаның деректері көрсетілсе, импорттау аяқталғаннан кейін тапсырманы ашып, құпиясөзді қайта енгізу қажет болады.

Импорттау сәтсіз болса, келесі әрекеттердің бірін орындауға болады:

- Басқару сервер иерархиясының қолдауы арқылы деректерді тасымалдау үшін экспорттық файлды қайта импорттауға болады.

- Басқару сервер иерархиясының қолдауынсыз деректерді тасымалдау үшін басқа экспорттау файлын таңдау мақсатында деректерді тасымалдау шеберін іске қосып, оны қайтадан импорттауға болады.

Экспорттау ауқымына кіретін топ нысандарының Kaspersky Security Center Linux жүйесіне сәтті импортталғанын тексеруге болады. Ол үшін **Активтер (құрылғылар)** бөліміне өтіп, импортталған нысандардың сәйкес бөлімшелерде көрсетілгеніне көз жеткізіңіз.

Импортталған басқарылатын құрылғылар **Басқарылатын құрылғылар** бөлімшесінде көрсетілетінін, бірақ олар желіде көрінбейтінін және желілік агент орнатылмағанын ескеріңіз (**Көзге көрінетін**, **Желілік агент орнатылған** бағандарындағы **Желілік агент іске қосулы** *Жоқ* мәні).

Деректерді тасымалдауды аяқтау үшін Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру қажет.

Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру

Басқарылатын құрылғылар, нысандар және олардың параметрлері туралы ақпаратты Kaspersky Security Center Linux жүйесіне сәтті импорттағаннан кейін, деректерді тасымалдауды аяқтау үшін Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру қажет.

Басқарылатын құрылғыларды Kaspersky Security Center Linux басқаруымен келесі жолдардың бірімен жылжытуға болады:

- klmover утилитасын пайдалану арқылы.
- *Басқару серверін өзгерту* тапсырмасын пайдалану.
- Сертификатты және Басқару сервердің жеке кілтін сақтық көшірмеден қалпына келтіру арқылы (тек Kaspersky Security Center Linux 15.1 және одан жоғары нұсқасына деректерді тасымалдау үшін).

  Қосымша ақпаратты деректерді тасымалдаудың негізгі сценарийінің 6-қадамынан қараңыз.
- Қашықтан орнату тапсырмасы көмегімен басқарылатын құрылғыларға желілік агентті орнату арқылы.

Желілік агентті орнату арқылы Kaspersky Security Center Linux басқаруындағы басқарылатын құрылғыларды ауыстыру үшін:

1. Kaspersky Security Center Linux басқаруына ауыстырылатын импортталған басқарылатын құрылғылардан Желілік агентті жойыңыз.
2. Kaspersky Security Center Windows Басқару серверіне ауысыңыз.
3. **Табу және орналастыру** →**Орналастыру және тағайындау** →**Орнату пакеттері** бөліміне өтіңіз және бар Желілік агентті орнату пакетінің сипаттарын ашыңыз.

   Желілік агентті орнату бумасы бумалар тізімінде болмаса, жаңасын жүктеп алыңыз.

   Сондай-ақ желілік агентті жергілікті түрде орнату үшін автономды орнату бумасын жасауға және пайдалануға болады.
4. **Параметрлер** қойыншасында **Қосылым** бөлімін таңдаңыз. Kaspersky Security Center Linux Басқару сервері үшін қосылым параметрлерін көрсетіңіз.
5. Импортталған басқарылатын құрылғылар үшін қашықтан орнату тапсырмасын жасаңыз, содан кейін қайта орнатылған желілік агентті орнату бумасын көрсетіңіз.

   Желілік агентті Kaspersky Security Center Windows Басқару серверін немесе тарату нүктесі ретінде әрекет ететін Windows жүйесімен жұмыс істейтін құрылғыны пайдаланып орнатуға болады. Басқару серверін пайдаланып жатсаңыз, **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен** параметрін қосыңыз. Тарату нүктесін пайдаланып жатсаңыз, **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен** параметрін қосыңыз.
6. Бағдарламаны қашықтан орнату тапсырмасын іске қосыңыз.

Қашықтан орнату тапсырмасын сәтті орындағаннан кейін, Kaspersky Security Center Linux Басқару серверіне өтіп, басқарылатын құрылғылар желіде көрінетініне және оларда желілік агент орнатылғанына және жұмыс істеп тұрғанына көз жеткізіңіз (**Көзге көрінетін**, **Желілік агент орнатылған** және **Желілік агент іске қосулы** бағандарындағы *Иә* мәні).

Kaspersky Security Center Web Console бағдарламасына кіру және одан шығу

Kaspersky Security Center Web Console веб-консоліне Басқару серверін және Kaspersky Security Center Web Console веб-консолін орнатқаннан кейін кіре аласыз. Сіз орнату барысында көрсетілген Басқару серверінің веб-мекенжайын білуіңіз қажет (әдепкі бойынша 8080-порт қолданылады). Сіздің браузеріңізде JavaScript қосулы болуы тиіс.

Kaspersky Security Center Web Console веб-консоліне келесі тәсілдердің бірімен кіруге болады:

- Домендік түпнұсқалық растамасын пайдалану арқылы.

  Бұл тәсілді таңдасаңыз, домен контроллерлерінің сауалнамасы қосылғанын және домен пайдаланушыларының басқару серверіне қосылғанын тексеріңіз.

- Доменнің пайдаланушы есептік жазбасының атауы мен құпиясөзін көрсету арқылы
- Әкімші есептік жазбасының аты мен құпиясөзін көрсету арқылы.

Kaspersky Security Center Web Console-ге кіргіңіз келетін Пайдаланушы есептік жазбасына рөл тағайындалған болуы керек. Кірмес бұрын, доменге немесе ішкі пайдаланушы есептік жазбасына рөл тағайындалғанына көз жеткізіңіз. Әйтпесе, кіру қатесі орын алады.

Домендік түпнұсқалық растамасын пайдаланып жүйеге кіру

Домендік түпнұсқалық растаманы қолдану арқылы Kaspersky Security Center Web Console веб-консоліне кіру үшін:

1. Браузеріңізде https://<`Kaspersky Security Center Web Console мекенжайы`>:<`Порт нөмірі`> бетіне өтіңіз

   Бағдарламаға кіру беті көрсетіледі.

2. Бірнеше сенімді Басқару серверін қосқан болсаңыз, тізімнен қосылғыңыз келетін Басқару серверін таңдаңыз.

   Тек бір басқару серверін қосқан болсаңыз, басқару серверлерінің тізімі көрсетілмейді.

3. Келесі әрекеттердің бірін орындаңыз:

   - **Домен аутентификациясын пайдалану** түймесін басыңыз.
   - Егер Серверде бір немесе бірнеше виртуалды Басқару сервері жасалған болса және сіз домендік түпнұсқалық растама арқылы виртуалды Серверге кіргіңіз келсе:

     a. **Виртуалды сервер опцияларын көрсету** түймесін басыңыз.

     b. Виртуалды Серверді жасау кезінде көрсетілген виртуалды Басқару сервері атауын енгізіңіз.

     c. **Домен аутентификациясын пайдалану** түймесін басыңыз.

4. Есептік жазбаңыз үшін екі сатылы тексеру қосылған болса, мобильдік құрылғыдағы аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіңіз.

   Қажет болса, кіру бетіне оралуға болады.

Жүйеге кіргеннен кейін, ақпараттық тақта сіз соңғы рет қолданған тіл және тақырыппен көрсетіледі. Сіз Kaspersky Security Center Web Console шарлай аласыз және оны Kaspersky Security Center бағдарламасымен жұмыс істеу үшін қолдана аласыз.

Әкімші есептік жазбасының аты мен құпиясөзі арқылы кіріңіз

Әкімші есептік жазбасының аты мен құпиясөзін көрсету арқылы Kaspersky Security Center Web Console жүйесіне кіру үшін:

1. Браузеріңізде https://<Kaspersky Security Center Web Console мекенжайы>:<Порт нөмірі> бетіне өтіңіз

   Бағдарламаға кіру беті көрсетіледі.

2. Бірнеше сенімді Басқару серверін қосқан болсаңыз, тізімнен қосылғыңыз келетін Басқару серверін таңдаңыз.

   Тек бір басқару серверін қосқан болсаңыз, басқару серверлерінің тізімі көрсетілмейді.

3. Келесі әрекеттердің бірін орындаңыз:

   - Басқару серверіне доменнің пайдаланушы есептік жазбасымен кіру үшін:

     a. Домен пайдаланушысының аты мен құпиясөзін енгізіңіз.

     Домен пайдаланушы атын келесі пішімдердің бірімен енгізуге болады:

     - `Пайдаланушы аты@dns.domain`
     - `NTDOMAIN\Пайдаланушы аты`

     b. **Кіру** түймесін басыңыз.

     Домен пайдаланушы тіркелгісімен жүйеге кірмес бұрын, домен пайдаланушыларының тізімін алу үшін домен контроллерлерінен сұраңыз.

- Басқару серверіне кіру үшін:

  a. Жергілікті әкімшінің пайдаланушы аты мен құпиясөзін енгізіңіз.

  b. **Кіру** түймесін басыңыз.

- Егер Серверде бір немесе бірнеше виртуалды Басқару сервері жасалған болса және сіз виртуалды Серверге кіргіңіз келсе:

  a. **Виртуалды сервер опцияларын көрсету** түймесін басыңыз.

  b. Виртуалды Серверді жасау кезінде көрсетілген виртуалды Басқару сервері атауын енгізіңіз.

  c. Виртуалды Басқару серверінде құқықтары бар әкімшінің пайдаланушы аты мен құпиясөзін енгізіңіз.

  d. **Кіру** түймесін басыңыз.

4. Есептік жазбаңыз үшін екі сатылы тексеру қосылған болса, мобильдік құрылғыдағы аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіңіз.

   Қажет болса, кіру бетіне оралуға болады.

5. Есептік жазбаңыз үшін құпиясөзді өзгертуге мәжбүрлеу қосылса немесе құпиясөз мерзімі өтіп кетсе, құпиясөзді өзгерту терезесі пайда болады. Kaspersky Security Center Web Console веб-консоліне кіруге арналған жаңа құпиясөзді орнатыңыз.

Жүйеге кіргеннен кейін, ақпараттық тақта сіз соңғы рет қолданған тіл және тақырыппен көрсетіледі. Сіз Kaspersky Security Center Web Console шарлай аласыз және оны Kaspersky Security Center бағдарламасымен жұмыс істеу үшін қолдана аласыз.

Шығу

Kaspersky Security Center Web Console веб-консолінен шығу үшін,

Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Шығу** тармағын таңдаңыз.

Kaspersky Security Center Web Console бағдарламасы жабық, бағдарламаға кіру беті көрсетіледі.

Kaspersky Security Center Web Console Есептік деректер және қатынасу диспетчері

Бұл бөлімде Есептік деректер және қатынасу диспетчері (бұдан әрі - IAM) туралы ақпарат берілген.

Есептік деректер және қатынасу диспетчері құрамдасы туралы

Есептік деректер және қатынасу диспетчері (бұдан әрі IAM деп те аталады) – бұл Kaspersky Security Center Web Console веб-консолі мен Kaspersky Industrial CyberSecurity for Networks веб-интерфейсі арасында бірыңғай кіруді (Single Sign-on, SSO) қолдануға мүмкіндік беретін Kaspersky Security Center Web Console құрамдасы. IAM құрамдасы Kaspersky Industrial CyberSecurity for Networks веб-интерфейсін Kaspersky Security Center Web Console веб-консолінде авторизациялану үшін OAuth 2.0 протоколын қолданады.

Бұл жағдайда, Kaspersky Security Center Web Console арқылы қатынасуға болатын Kaspersky Industrial CyberSecurity for Networks бағдарламасы *ресурстар сервері* деп, ал Kaspersky Security Center Web Console және Kaspersky Industrial CyberSecurity for Networks веб-интерфейсі – *OAuth 2.0 клиенттері* деп аталады. Ресурстар сервері – бірнеше пайдаланушымен жұмыс істейтін және авторизацияны талап ететін бағдарлама. Клиент ресурстар серверінде авторизациядан өту үшін *токен* ді қолданады. Токен – байттардың бірегей тізбегі. Токеннің жарамдылық мерзімі аяқталғаннан кейін, ол автоматты түрде қайта шығарылады. IAM құрамдасы OAuth 2.0 бірнеше клиенттері үшін бірыңғай авторизация сервері ретінде әрекет етеді.

Kaspersky Security Center Web Console орнату кезінде IAM орнатуға болады. Оны кейінірек Kaspersky Security Center Web Console параметрлерінде кез келген уақытта қосуға болады. Егер Kaspersky Industrial CyberSecurity сервері немесе Kaspersky Industrial CyberSecurity веб-интерфейсі сол Басқару сервері басқаратын құрылғыға орнатылса, IAM бұл бағдарламаны анықтайды және Kaspersky Security Center Web Console сервері бұл туралы хабарландыруды көрсетеді. Сіз Kaspersky Industrial CyberSecurity for Networks тіркей аласыз, содан соң SSO бірыңғай кіруін Kaspersky Security Center Web Console үшін де, Kaspersky Industrial CyberSecurity for Networks веб-интерфейсі үшін де қолдана аласыз.

Kaspersky Security Center Web Console веб-консолінен шықсаңыз, Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіндегі сеансыңыз аяқталады және сізге Kaspersky Security Center Web Console веб-консолінің қайта кіруге тура келеді.

Есептік деректер және қатынасу диспетчерін қосу: сценарий

Алдын ала талаптар

Жұмысты бастамас бұрын, Kaspersky Industrial CyberSecurity for Networks веб-интерфейсінің 3.1 немесе одан да жаңа нұсқасына қатынасу мүмкіндігіңіз бар екеніне көз жеткізіңіз.

Кезеңдер

Есептік деректер және қатынасу диспетчерін (IAM деп те аталады) қосу кезең-кезеңімен жүзеге асырылады:

1. **Қажетті порттарды тексеру**

   Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыда 3333, 4004 және 4444 порттары ашық екеніне көз жеткізіңіз. Бұл порттар OAuth 2.0 пайдалану үшін қажет. Әдепкі бойынша порт нөмірлерін Kaspersky Security Center Web Console параметрлері терезесінде өзгертуге болады.

   3333, 4004 және 4444 порттарынан басқа, Kaspersky Security Center Web Console сервері 4445, 2444 және 2445 порттарын әртүрлі мақсаттарда пайдаланады.

2. **Есептік деректер және қатынасу диспетчерін орнату**

   Kaspersky Security Center Web Console серверін орнату барысында Есептік деректер және қатынасу диспетчерін орнатқыңыз келетінін көрсетіңіз. Егер олай болмаса, Kaspersky Security Center Web Console веб-консолін орнату шеберін қайтадан іске қосыңыз.

3. **Есептік деректер және қатынасу диспетчерін конфигурациялау**

   Kaspersky Security Center Web Console параметрлері терезесінде **Есептік деректер және қатынасу диспетчері (IAM)** қосқышының қосулы екеніне көз жеткізіңіз. Сондай-ақ, Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғының DNS атауын көрсетіңіз: клиенттік бағдарламалар осы құрылғыға қосылады.

4. **Токен параметрлерін көрсету**

   Kaspersky Security Center Web Console параметрлері терезесінде Есептік деректер және қатынасу диспетчерін қолданатын токендердің өміршеңдік уақытын және авторизацияны күту уақытын көрсетіңіз. Сіз әдепкі бойынша мәндерді қолдана аласыз немесе өз қажеттіліктеріңізге сәйкес мәндеріңізді көрсете аласыз.

5. **Сертификаттарды ұсыну**

   Басқару сервері жасаған сертификаттарды пайдаланғыңыз келсе, Kaspersky Security Center Web Console параметрлер терезесінде IAM пайдаланатын порттардың түбірлік сертификаттарын жүктеп алып, оларды Kaspersky Security Center Web Console пайдаланушыларының жұмыс станцияларына таратыңыз. Әйтпесе, пайдаланушы браузерлері Kaspersky Security Center Web Console веб-консолін қосылуға әрекеттену кезінде қате туралы хабарларды көрсетеді.

6. **Kaspersky Industrial CyberSecurity for Networks серверлерін және Kaspersky Industrial CyberSecurity for Networks веб-интерфейстерін тіркеу**

   IAM диспетчерін Kaspersky Security Center Web Console веб-консолін орнатқан кезде Industrial CyberSecurity for Networks сервері (немесе бірнеше Сервер) және бір немесе бірнеше Kaspersky Industrial CyberSecurity for Networks веб-интерфейсі тіркелуді күтетіні туралы хабар көрсетіледі. Kaspersky Industrial CyberSecurity for Networks Server серверін (немесе серверлерін) және веб-интерфейсті (немесе веб-интерфейстерді) тіркеу үшін осы хабарды басыңыз.

Нәтижелер

Осы сценарий аяқталғаннан кейін, сіз Kaspersky Industrial CyberSecurity for Networks және Kaspersky Security Center Web Console үшін SSO және IAM қолдана аласыз.

Kaspersky Security Center Web Console Есептік деректер және қатынасу диспетчерін конфигурациялау

Есептік деректер және қатынасу диспетчерін өз талаптарыңызға сай конфигурациялау үшін:

1. Негізгі мәзірден **Параметрлер** → **Есептік деректер және қатынасу диспетчері** тармағына өтіңіз.
2. **Есептік деректер және қатынасу диспетчері** бөлімінде Есептік деректер және қатынасу диспетчері қосулы екеніне көз жеткізіңіз.
3. **Параметрлер** сілтемесі арқылы **Есептік деректер және қатынасу диспетчерінің желі атауы** блогына өтіңіз.
4. Сіз Есептік деректер және қатынасу диспетчерін орнатқан құрылғының DNS атауын көрсетіңіз. Клиенттік бағдарламалар осы құрылғыға қосылады.
5. Қаласаңыз, тиісті параметрлер тобының астындағы **Параметрлер** сілтемесін басу арқылы әдепкі бойынша токен параметрлерін, сертификат параметрлерін, сондай-ақ порт нөмірлерін өзгертіңіз.

Есептік деректер және қатынасу диспетчері қосылған және сіздің талаптарыңызға сай жұмыс істейді.

Kaspersky Security Center Web Console веб-консолінде Kaspersky Industrial CyberSecurity for Networks бағдарламаларын тіркеу

Kaspersky Industrial CyberSecurity for Networks бағдарламасымен Kaspersky Security Center Web Console арқылы жұмысты бастау үшін оны алдын ала Kaspersky Security Center Web Console веб-консолінде тіркеу керек.

Kaspersky Industrial CyberSecurity for Networks бағдарламасын тіркеу үшін:

1. Келесі әрекеттердің орындалғанына көз жеткізіңіз:
   - Сіз Kaspersky Industrial CyberSecurity for Networks веб-плагинін жүктеп алып, орнаттыңыз.

     Мұны кейінірек, Kaspersky Industrial CyberSecurity for Networks серверінің Басқару серверімен синхрондалуын күте отырып, орындауға болады.
   - Сіз бірыңғай кіру (SSO) технологиясын қолдануға дайындау сценарийін аяқтадыңыз.
   - Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіндегі қажетті параметрлер Kaspersky Security Center бетінде белгіленген. Толық ақпарат Kaspersky Industrial CyberSecurity for Networks онлайн-анықтамасында келтірілген.
   - Сіз Kaspersky Security Center Web Console веб-консолінe әкімшінің есептік жазбасымен кірдіңіз.
   - IAM конфигурацияланған.

2. Kaspersky Industrial CyberSecurity for Networks сервері орнатылған құрылғыны Тағайындалмаған құрылғылар тобынан Басқарылатын құрылғылар тобына жылжытыңыз:

   a. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Тағайындалмаған құрылғылар** бөліміне өтіңіз.

   b. Kaspersky Industrial CyberSecurity for Networks Server орнатылған құрылғының жанына жалауша қойыңыз.

   c. **Топқа жылжыту** түймесін басыңыз.

   d. Басқару топтарының иерархиясында Басқарылатын құрылғылар тобының жанына жалауша қойыңыз.

   e. **Жылжыту** түймесін басыңыз.

3. Kaspersky Industrial CyberSecurity for Networks сервері орнатылған құрылғының сипаттарына өтіңіз.

4. Құрылғы сипаттары терезесінде, **Жалпы** бөлімінде **Басқару серверімен байланысты үзбеу** параметрін таңдаңыз, содан соң **Сақтау** түймесін басыңыз.

5. Құрылғы сипаттары терезесінде **Бағдарламалар** бөлімін таңдаңыз.

6. **Бағдарламалар** бөлімінде Желілік агентті таңдаңыз.

7. Бағдарламаның ағымдағы күйі *Тоқтатылды* болса, ол *Орындалуда* күйіне өзгергенше күтіңіз.

   Бұл 15 минутқа дейін созылуы мүмкін. Kaspersky Industrial CyberSecurity for Networks веб-плагинін әлі орнатпаған болсаңыз, оны дәл қазір, күтіп тұрған кезде жасай аласыз.

8. Негізгі мәзірден **Параметрлер** → **Есептік деректер және қатынасу диспетчері** тармағына өтіңіз.

   Тіркеуге сұрау салу өрісінде бір күтіп тұрған сұрау көрсетіледі.

9. **Тіркеуге сұрау салу** өрісінен төмен орналасқан **Параметрлер** сілтемесінен өтіңіз.

10. Тіркелген клиенттер тізімі ашылғанда, *Күштеп қолдану күтілуде* күйі бар Kaspersky Industrial CyberSecurity for Networks сервері атауының жанына жалауша қойыңыз, содан соң **Бекіту** түймесін басыңыз.

    Kaspersky Industrial CyberSecurity for Networks серверін тіркегіңіз келмесе, Қабылдамау түймесін басып, осы тізімге кейінірек оралуға болады.

    Бекіту түймесін басқаннан кейін, күйі *Расталды*, содан соң *Дайын* күйіне өзгереді. Егер күй өзгермеген болса, Жаңарту түймесін басуға болады.

11. Тіркелген клиенттер тізімін жауып, **Тіркелген клиенттер** өрісіндегі мән ұлғайғанына көз жеткізіңіз.

12. Басқару тақтасына Kaspersky Industrial CyberSecurity for Networks веб-виджетін қосу үшін:

    a. Негізгі мәзірдегі **Бақылау және есеп беру** → **Бақылау тақтасы** тармағына өтіңіз.

    b. Басқару тақтасында **Веб-виджетті қосу не қалпына келтіру** түймесін басыңыз.

    c. Пайда болған веб-виджетте **Басқа** түймесін басыңыз.

    d. Kaspersky Industrial CyberSecurity for Networks виджетін таңдаңыз.

Енді сіз веб-виджеттегі сілтеме арқылы Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіне өте аласыз.

Тіркелу рәсімі аяқталғаннан кейін, Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіне кіру бетінде көрсетілетін **Kaspersky Security Center** жаңа түймесі пайда болады. Kaspersky Security Center есептік деректерінің астындағы Kaspersky Industrial CyberSecurity for Networks веб-интерфейсіне кіру үшін осы түймені басуға болады.

Есептік деректер және қатынасу диспетчері үшін авторизацияны күту уақыты және токендердің өміршеңдік уақыты

Есептік деректер және қатынасу диспетчері (бұдан әрі - IAM) құрамдасын конфигурациялау кезінде токеннің өміршеңдік уақыты мен авторизацияны күту уақыты параметрлерін көрсету қажет. Әдепкі бойынша параметрлер қауіпсіздік стандарттарын да, Серверге түсетін жүктемені де ескере отырып әзірленген. Сіз бұл параметрлерді ұйымыңыздың саясатына сәйкес өзгерте аласыз.

IAM диспетчері, мерзімі аяқталған токенді автоматты түрде қайта шығарады.

Төмендегі кестеде токеннің әдепкі бойынша өміршеңдік уақыты параметрлері келтірілген.

Токеннің өміршеңдік уақытының параметрлері

Токен	Әдепкі бойынша өміршеңдік уақыты (секундтарда)	Сипаттамасы
Сәйкестілік куәлігінің таңбалауышы (id_token)	86400	OAuth 2.0 клиенті пайдаланатын сәйкестендіру токені (яғни, Kaspersky Security Center Web Console немесе Kaspersky Industrial CyberSecurity веб-интерфейсі). IAM клиентке пайдаланушы туралы ақпаратты (яғни пайдаланушы профилін) қамтитын токен идентификаторын жібереді.
Қатынасу таңбалауышы (access_token)	86400	OAuth 2.0 клиенті IAM анықтаған ресурс иесінің атынан ресурстар серверіне қатынасу үшін пайдаланатын қатынасу токені.
Жаңарту таңбалауышы (refresh_token)	172800	OAuth 2.0 клиенті бұл таңбалауышты сәйкестендіру токенін және қатынасу токенін қайта беру үшін пайдаланады.

Төмендегі кестеде auth_code және login_consent_request үшін күту уақыты келтірілген.

Авторизацияны күту уақыты параметрлері

Параметр	Әдепкі бойынша күту уақыты (секунд түрінде)	Сипаттамасы
Авторизация коды (auth_code)	3600	Токен кодының айырбасталуын күту уақыты. OAuth 2.0 клиенті бұл кодты ресурстар серверіне жібереді және оның орнына қатынасу токенін алады.
Жүйеге кіру келісімін сұраудың күту уақыты (login_consent_request)	3600	OAuth 2.0 клиентіне пайдаланушы құқығын табыстау үшін күту уақыты.

Токендер туралы қосымша ақпарат алу үшін OAuth веб-сайтын қараңыз.

Тінтуір немесе пернетақта әрекеті анықталмаған клиенттер үшін күту уақытын конфигурациялау үшін:

1. Kaspersky Security Center Web Console орнату қалтасында config.json файлын тауып, ашыңыз. Файлда клиенттің әрекетсіздік күту уақытын реттеуге арналған параметрлер бар.

2. Белсенді емес клиентке қалқымалы ескертуді көрсеткенге дейін уақытты миллисекундпен көрсету үшін `clientIdleTimeout` параметрін пайдаланыңыз.

3. Белсенді емес клиент үшін IAM авторизациясының аяқталуына дейінгі уақытты миллисекундпен көрсету үшін `clientLogoutTimeout` параметрін пайдаланыңыз. `clientLogoutTimeout` параметрінің мәні `clientIdleTimeout` параметрінен кейін ретпен есептеледі.

IAM сертификаттарын жүктеу және тарату

Әдепкі бойынша, Есептік деректер және қатынасу диспетчері браузерлерге Kaspersky Security Center Web Console бағдарламасына қатынасуға мүмкіндік беру үшін Басқару сервері жасаған сертификаттарды пайдаланады. Сондай-ақ, пайдаланушы сертификаттарын пайдалана аласыз. Қандай сертификатты пайдалансаңыз да, Kaspersky Security Center Web Console пайдаланушылары Kaspersky Security Center Web Console веб-консоліне жүгінетін барлық жұмыс станциялары осы сертификатқа сенетініне көз жеткізуіңіз керек.

Сертификаттарды жүктеу және тарату үшін:

1. Негізгі мәзірден **Параметрлер** → **Есептік деректер және қатынасу диспетчері** тармағына өтіңіз.

2. Әр сертификат үшін тиісті параметрлер тобының астындағы **Конфигурациялар** сілтемесін нұқыңыз және келесі әрекеттердің бірін орындаңыз:

   - Kaspersky Security Center Web Console орнату кезінде Басқару сервері жасаған сертификатты пайдаланғыңыз келсе:

     1. Ашылған сертификат сипаттары терезесінде **Басқару сервері жасаған сертификатты** таңдаңыз.

     2. Сертификатты жүктеу үшін **Жүктеу** түймесін басыңыз.

     3. Жүктелген сертификатты Kaspersky Security Center Web Console пайдаланушылары Kaspersky Security Center Web Console серверіне қатынаса алатын барлық жұмыс станцияларына таратыңыз.

   - Егер сізде пайдаланғыңыз келетін сертификат болса:

     1. Сертификат сипаттарының ашылған терезесінде **Пайдаланушы TLS сертификаты** тармағын таңдаңыз.

     2. Сертификат файлы мен жеке кілтті таңдаңыз.

     3. **OK** түймесін басыңыз.

     4. Пайдаланушылар Kaspersky Security Center Web Console веб-консоліне немесе Kaspersky Industrial CyberSecurity веб-интерфейсіне қатынаса алатын барлық жұмыс станцияларына сертификатты таратыңыз.

Сертификаттар пайдаланушыларға Kaspersky Security Center Web Console веб-консоліне және Kaspersky Industrial CyberSecurity веб-интерфейсіне қатынасуға мүмкіндік береді.

Сізге барлық сертификаттарды уақтылы қайта шығару қажет. Басқару сервері жасаған сертификаттар қолмен қайта жасалуы керек. Kaspersky Security Center Web Console орнатушысы жасаған сертификаттар орнатушының көмегімен қайта жасалуы керек.

Есептік деректер және қатынасу диспетчерін өшіру

Есептік деректер және қатынасу диспетчерін (IAM) өшіре аласыз.

IAM өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Параметрлер** → **Біріктіру** бөліміне өтіңіз.
2. **Есептік деректер және қатынасу диспетчері** бөлімінде **Есептік деректер және қатынасу диспетчері** қосқышын өшірулі күйге орнатыңыз.

IAM диспетчерін кейінірек кез келген уақытта қосуға болады.

Егер сіз Kaspersky Security Center Web Console бағдарламасын орнатушы арқылы жаңартсаңыз және IAM орнатқыңыз келмейтінін көрсетсеңіз, онда Kaspersky Security Center Web Console жаңартылады, ал IAM орнатылмайды. Құрылғыңыздан мыналар жойылады: Kaspersky Industrial CyberSecurity for Networks веб-интерфейсімен біріктіру туралы барлық ақпарат, IAM конфигурация файлдары және журнал файлдары.

NTLM және Kerberos протоколдарын қолдана отырып, домендік түпнұсқалық растаманы конфигурациялау

Kaspersky Security Center 15.1 бағдарламасы NTLM және Kerberos протоколдары арқылы OpenAPI интерфейсінде домендік түпнұсқалық растаманы пайдалануға мүмкіндік береді. Домендік түпнұсқалық растаманы пайдалану Windows пайдаланушысына корпоративтік желіде құпиясөзді қайта енгізбей (бірыңғай кіру), Kaspersky Security Center Web Console серверінде қауіпсіз түпнұсқалық растаманы қосуға мүмкіндік береді.

Kerberos протоколы бойынша OpenAPI интерфейсіндегі домендік түпнұсқалық растаманың келесі шектеулері бар:

- Kaspersky Security Center Web Console пайдаланушысы Kerberos протоколы бойынша Active Directory-да түпнұсқалық растамадан өтуі тиіс. Пайдаланушының Kerberos мандаттарын (бұдан әрі – TGT) беруге жарамды мандаты болуы керек. TGT, домендік түпнұсқалық растама кезінде автоматты түрде шығарылады.
- Kerberos аутентификациясын браузерде реттеуіңіз керек. Толығырақ сіз қолданатын браузердің құжаттамасынан қараңыз.

Егер сіз Kerberos протоколдарын қолдана отырып, домендік түпнұсқалық растаманы қолданғыңыз келсе, сіздің желіңіз келесі шарттарға сай болуы керек:

- Басқару сервері домендік есептік жазбаның астында іске қосылуы қажет.
- Kaspersky Security Center Web Console сервері Басқару серверімен бір құрылғыда орнатылған.

- Басқару серверінің есептік жазбасы үшін келесі қызмет субъектілерінің аттарын (SPN) көрсету қажет:
  - "http/<server.fqnd.name>"
  - "http/<server>"

  Мұндағы <server> – Басқару сервері құрылғысының желілік атауы, <server.fqnd.name> – Басқару сервері құрылғысының толық домендік атауы.
- Басқару консолі немесе Kaspersky Security Center Web Console сервері арқылы қосылған кезде Басқару серверінің мекенжайын субъект-қызмет (SPN) аты тіркелген мекенжай сияқты көрсету қажет. Сіз <server.fqnd.name> немесе <server> мекенжайын көрсете аласыз.
- Құпиясөзсіз кіру үшін Kaspersky Security Center Web Console ашылған браузер процесі домендік есептік жазба астында жұмыс істеуі керек.

Kerberos және NTLM протоколдарына тек Kaspersky Security Center 15.1 үшін OpenAPI интерфейсінде қолдау көрсетіледі. Бұл протоколдарға Kaspersky Security Center Linux үшін OpenAPI интерфейсінде қолдау көрсетілмейді.

Басқару серверін конфигурациялау

Бұл бөлімде Басқару серверін конфигурациялау процесі мен сипаттары сипатталған.

Kaspersky Security Center Web Console веб-консолін Басқару серверіне қосу параметрлерін конфигурациялау

Басқару серверіне қосылу порттарын белгілеу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. **Жалпы** қойыншасында **Қосылу порттары** бөлімін таңдаңыз.

Қолданбада таңдалған серверге қосылудың негізгі параметрлері көрсетіледі.

Kaspersky Security Center Web Console веб-консолі Басқару серверіне TCP 13299 SSL-порты арқылы қосылған. Дәл осы портты klakaut автоматтандыру нысандары қолдануы мүмкін.

TCP 14000 порты Kaspersky Security Center Web Console веб-консолін, тарату нүктелерін, қосалқы Басқару серверлерін және klakaut утилитасының автоматтандыру нысандарын қосу, сондай-ақ клиент құрылғыларынан деректер алу үшін пайдаланылуы мүмкін.

Әдетте, TCP 13000 SSL портын тек Желілік агент, қосалқы Сервер және демилитаризацияланған аймақта орналасқан басты Басқару сервері ғана қолдана алады. Кейбір жағдайларда Kaspersky Security Center Web Console веб-консолін 13000 SSL-порты арқылы қосу қажет болуы мүмкін:

- Kaspersky Security Center Web Console үшін де, басқа белсенділіктер үшін де бірдей SSL портын қолданған жөн болса (клиент құрылғыларынан деректерді алу, тарату нүктелерін қосу, қосалқы Басқару серверлерін қосу үшін);
- егер klakaut утилитасын автоматтандыру нысаны Басқару серверіне тікелей емес, демилитаризацияланған аймақта орналасқан тарату нүктесі арқылы қосылса.

Басқару серверіне қосылу оқиғасының журналын реттеу

Басқару серверінің жұмысы барысында, оған қосылымдар мен қосылым әрекеттері тарихын журнал файлына сақтауға болады. Файлдағы ақпарат желі инфрақұрылымы ішіндегі қосылымдарды ғана емес, серверлерге рұқсатсыз қатынасу әрекеттерін де қадағалауға мүмкіндік береді.

Басқару серверіне қосылым оқиғаларын тіркеуді конфигурациялау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Қосылу порттары** бөлімін таңдаңыз.
3. **Басқару серверінің байланыс оқиғаларын журналға тіркеу** параметрін қосыңыз.

Басқару серверіне кіріс қосылымдарының барлық кейінгі оқиғалары, түпнұсқалық растама нәтижелері және SSL қателері %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog файлына жазылатын болады.

Басқару серверінің интернетке қатынасу параметрлерін конфигурациялау

Kaspersky Security Network пайдалану, сондай-ақ Kaspersky Security Center және Kaspersky басқарылатын бағдарламалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.

Басқару серверінің интернетке қатынасу параметрлерін көрсету үшін:

1. Басты мәзірде Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Интернет желісіне қатынасу параметрлері** бөлімін таңдаңыз.
3. Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін қосыңыз. Параметр қосулы болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

   - **Мекенжай**

     Kaspersky Security Center-ді интернетке қосу үшін прокси-сервер мекенжайы.

- **Порт нөмірі**

  Kaspersky Security Center прокси-қосылымы орнатылатын порт нөмірі.

- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Жергілікті желідегі құрылғыларға қосылған кезде прокси-сервер қолданылмайды.

- **Прокси-сервердегі түпнұсқалық растама**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

- **Пайдаланушы аты**

  Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Сондай-ақ, бағдарламаны жылдам іске қосу шебері арқылы интернетке қатынасуды конфигурациялуға болады.

Оқиғалар қоймасындағы оқиғалар санын конфигурациялау

Басқару сервері сипаттары терезесінің **Оқиғалар қоймасы** бөлімінде Басқару серверінің дерекқорында оқиғаларды сақтау параметрлерін конфигурациялауға болады: оқиғалар туралы жазбалар санын және жазбаларды сақтау уақытын шектеу. Оқиғалардың ең көп санын көрсеткенде, бағдарламалар оқиғалардың көрсетілген санын сақтау үшін диск кеңістігінің долбарлы өлшемін есептейді. Сіз бұл есептеуді дерекқордың толып кетуіне жол бермеу үшін бос диск кеңістігінің жеткілікті ме екенін бағалау үшін пайдалана аласыз. Әдепкі бойынша, Басқару сервері дерекқорының сыйымдылығы 400 000 оқиғаны құрайды. Дерекқордың ұсынылған ең жоғары сыйымдылығы 45 000 000 оқиғаны құрайды.

Бағдарлама дерекқорды 10 минут сайын тексереді. Оқиғалар саны көрсетілген максималды мәннен 10 000 артық болса, бағдарлама оқиғалардың көрсетілген ең көп саны ғана қалуы үшін ең ескі оқиғаларды жояды.

Басқару сервері ескі оқиғаларды жойған кезде, ол жаңа оқиғаларды дерекқорға сақтай алмайды. Осы кезең ішінде қабылданбаған оқиғалар туралы ақпарат Kaspersky Event журналына жазылады. Жаңа оқиғалар кезекке қойылады, содан соң жою операциясы аяқталғаннан кейін, дерекқорда сақталады.

Басқару серверіндегі оқиғалар қоймасында сақтауға болатын оқиғалар санын шектеу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Оқиғалар қоймасы** бөлімін таңдаңыз. Дерекқорда сақталатын оқиғалардың максималды санын көрсетіңіз.

3. **Сақтау** түймесін басыңыз.

Сондай-ақ келесі әрекеттерді орындауға болады:

- Тапсырманы орындау барысына қатысты оқиғаларды сақтау немесе тек тапсырманы орындау нәтижелерін сақтау үшін кез келген тапсырманың параметрлерін өзгертуге болады.
- Басқарылатын құрылғыларда орнатылған басқару сервері, желілік агент және Kaspersky қолданбаларының оқиғалары үшін сақтау мерзімін азайтуға немесе өшіруге болады.

Осылайша, сіз дерекқордағы оқиғалардың санын азайтасыз, дерекқордағы оқиғалар кестесін талдаумен байланысты сценарийлердің жұмыс жылдамдығын арттырасыз және критикалық оқиғаларды оқиғалардың көп санымен ығыстыру қаупін азайтасыз.

UEFI деңгейлі қорғанысты құрылғыларды қосу параметрлері

UEFI деңгейлі қорғанысты құрылғы – бұл BIOS деңгейінде кіріктірілген, UEFI үшін "Kaspersky" шешімі немесе бағдарламасы бар құрылғы. Кіріктірілген қорғаныс жүйені іске қосуды бастаған сәттен бастап құрылғының қауіпсіздігін қамтамасыз етеді, ал кіріктірілген БҚ жоқ құрылғылар қорғанысы тек қауіпсіздік бағдарламасы іске қосылғаннан кейін ғана әрекет ете бастайды. Kaspersky Security Center бағдарламасы осындай құрылғыларды басқаруға қолдау көрсетеді.

UEFI деңгейлі қорғанысты құрылғыларын қосу параметрлерін өзгерту үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Қосымша порттар** бөлімін таңдаңыз.

3. Қажетті параметрлерді өзгертіңіз:

   - **UEFI деңгейлі қорғанысты және KasperskyOS құрылғылары үшін портты ашу**

     UEFI деңгейлі қорғанысты құрылғылар Басқару серверіне қосыла алады.

   - **UEFI деңгейлі қорғанысты және KasperskyOS құрылғыларына арналған порт**

     UEFI деңгейлі қорғанысты және KasperskyOS құрылғылары үшін портты ашу нұсқасы таңдалса, порт нөмірін өзгертуге болады. Әдепкі бойынша 13294-порт орнатылған.

4. **Сақтау** түймесін басыңыз.

UEFI деңгейлі қорғанысты құрылғылар Басқару серверіне қосыла алады.

Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу

Қосалқы Басқару серверін қосу (болашақ негізгі Басқару серверімен бірге орындалады)

Басқару серверін қосалқы Сервер ретінде қосып, осылайша "басты Сервер – қосалқы Сервер" иерархиясының қатынасын орнатуға болады.

Kaspersky Security Center Web Console арқылы қосылуға болатын Басқару серверін қосалқы Сервер ретінде қосу үшін:

1. Болашақ басты Сервердің 13000-порты қосалқы Басқару серверлерінен қосылымдарды қабылдау үшін қолжетімді екеніне көз жеткізіңіз.
2. Болашақ негізгі Басқару серверінде параметрлер ( ) белгішесін басыңыз.
3. Ашылған сипаттар бетінде **Басқару серверлері** қойыншасына өтіңіз.
4. Басқару серверін қосқыңыз келетін басқару тобы атауының жанындағы жалаушаны қойыңыз.
5. Мәзірден **Қосалқы Басқару серверіне қосылу** тармағын таңдаңыз.

   Қосалқы Басқару серверін қосу шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
6. Келесі өрістерді толтырыңыз:

   - **DMZ режимінде негізгі Басқару серверін қосалқы Басқару серверіне қосу**

     Қосалқы Басқару сервері демилитаризацияланған аймақта (DMZ) болса, осы параметрді таңдаңыз.

     Бұл параметр таңдалған болса, сіз **Қосалқы Сервер мекенжайын** көрсетуіңіз керек.

     Егер бұл параметр таңдалса, негізгі Басқару сервері қосалқы Басқару серверіне қосылуды бастайды. Әйтпесе, қосалқы Басқару сервері негізгі Басқару серверіне қосылуды бастайды.

   - **Қосалқы Басқару серверінің көрсетілетін атауы**

     Серверлер иерархиясында көрсетілетін қосалқы Басқару серверінің атауы. Сіз IP мекенжайын атау ретінде енгізе аласыз немесе мысалы, "1-топқа арналған қосалқы Сервер" сияқты атауды қолдана аласыз.

   - **Қосалқы Басқару серверінің мекенжайы (міндетті емес)**

     Қосалқы Басқару серверінің IP мекенжайын немесе домен атауын көрсетіңіз.

     Бұл параметр **Демилитаризацияланған аймақтағы негізгі Серверді қосалқы Серверге қосу** параметрі қосылған болса қажет.

   - **Басқару сервері SSL порты**

     Иерархияны құрғаннан кейін негізгі және қосалқы Басқару серверлері арасындағы өзара әрекеттесу үшін пайдаланылатын SSL портының нөмірін көрсетіңіз. Әдепкі бойынша 13000-порт орнатылған.

   - **Басқару сервері API порты**

     Web Console OpenAPI арқылы қосалқы Басқару серверінен қосылымдарды алу үшін пайдаланатын порттың нөмірі. Әдепкі бойынша 13299-порт орнатылған.

     Иерархияны құру кезінде Web Console болашақ қосалқы Басқару серверіне қосылады, тіркелгі деректерін сұрайды, ашық сертификатты алады және бастапқы орнатуды орындайды.

     Басқару серверінің иерархиясы құрылғаннан кейін, 13299 порты енді пайдаланылмайды. Басқару серверлері 13000 порты арқылы өзара әрекеттеседі.
7. Қосалқы басқару серверінің сертификатын көрсетіңіз. Сертификат алу үшін **Қосалқы сервер мекенжайы** параметрін көрсетсеңіз, **Қосалқы басқару серверінен алу** түймесін басыңыз. Немесе **Сертификат файлын таңдау** түймесін басып, сертификат файлын шолыңыз.

8. Қосылым параметрлерін белгілеңіз:

   - Болашақ негізгі Басқару серверінің мекенжайын енгізіңіз.
   - Егер болашақ қосалқы Басқару сервері прокси-серверді пайдаланса, прокси-серверге қосылу үшін прокси-сервер мекенжайын және пайдаланушы есептік деректерін енгізіңіз.

9. Болашақ қосалқы Басқару серверіне кіру құқығы бар пайдаланушының есептік деректерін енгізіңіз.

10. Екі қадамдық тексеру қосылып, конфигурацияланса, аутентификация қолданбасы жасаған қауіпсіздік кодын беріңіз.

    Екі қадамдық тексеру қосылып, бірақ сіз көрсеткен есептік жазба үшін конфигурацияланбаған болса, тек болашақ қосалқы Серверден иерархия жасаңыз (төмендегі нұсқауларды қараңыз).

Егер қосылым параметрлері дұрыс болса, болашақ қосалқы Сервермен байланыс орнатылып, "негізгі/қосалқы" иерархиясы құрылады. Егер қосылым сәтсіз болса, қосылым параметрлерін тексеріңіз немесе болашақ қосалқы Сервердің сертификатын қолмен көрсетіңіз.

Негізгі және қосалқы Басқару серверлері арасындағы байланыс 13000-порт арқылы орнатылады. Негізгі Басқару серверінің тапсырмалары мен саясаттары алынды және қолданылды. Қосалқы Басқару сервері негізгі Басқару серверінде, ол қосылған басқару тобында көрсетіледі.

Қосалқы Басқару серверін қосу (болашақ қосалқы Басқару серверімен бірге орындалады)

Егер сіз болашақ қосалқы Басқару серверіне қосыла алмасаңыз (мысалы, ол уақытша өшірілген немесе қолжетімді емес болғандықтан), сіз әлі де қосалқы Басқару серверін қоса аласыз.

Kaspersky Security Center Web Console арқылы қосылуға қолжетімді емес Басқару серверін қосалқы Сервер ретінде қосу үшін:

1. Болашақ негізгі Басқару сервері сертификатының файлын болашақ қосалқы Басқару сервері орналасқан кеңсенің жүйелік әкімшісіне жіберіңіз. (Мысалы, файлды сыртқы құрылғыға жазуға немесе электрондық пошта арқылы жіберуге болады.)

   Сертификат файлы болашақ негізгі Басқару серверінде %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer мекенжайы бойынша орналасқан.

2. Болашақ қосалқы Басқару серверіне жауапты жүйелік әкімшіге мыналарды ұсыныңыз:

   a. Параметрлер белгішесін ( ) басыңыз.

   b. Ашылған сипаттар бетінде **Жалпы** қойыншасындағы **Басқару серверлерінің иерархиясы** бөліміне өтіңіз.

   c. **Бұл Басқару сервері иерархияда қосымша** параметрін таңдаңыз.

   d. **Негізгі Басқару серверінің мекенжайы** өрісінде болашақ негізгі Басқару серверінің желілік атауын енгізіңіз.

   e. **Шолу** түймесін басу арқылы болашақ негізгі Сервердің бұған дейін сақталған сертификат файлын таңдаңыз.

f. Қажет болса, **DMZ режимінде негізгі Басқару серверін қосалқы Басқару серверіне қосу** белгішесін қойыңыз.

g. Егер болашақ қосалқы Басқару серверіне қосылу прокси-сервер арқылы орындалса, **Прокси-серверді пайдалану** параметрін таңдап, қосылым параметрлерін белгілеңіз.

h. **Сақтау** түймесін басыңыз.

"Басты Сервер – қосалқы Сервер" қатынасы орнатылады. Басты Сервер 13000-портты пайдаланып қосалқы Серверден қосылымды қабылдай бастайды. Негізгі Басқару серверінің тапсырмалары мен саясаттары алынды және қолданылды. Қосалқы Басқару сервері негізгі Басқару серверінде, ол қосылған басқару тобында көрсетіледі.

Қосалқы Басқару серверлері тізімін қарау

Басқару серверлерінің (соның ішінде виртуалды) тізімін көру үшін:

Басты мәзірде параметрлер ( ) белгішесінің жанында орналасқан Басқару сервері атауын басыңыз.

Қосалқы (виртуалды) Басқару серверлерінің ашылмалы тізімі көрсетіледі.

Осы Басқару серверлерінің кез келгеніне оның атын басу арқылы өтуге болады.

Басқару топтары да көрсетіледі, бірақ олар белсенді емес және бұл мәзірде басқару үшін қолжетімді емес.

Егер сіз Kaspersky Security Center Web Console веб-консоліндегі негізгі Басқару серверіне қосылған болсаңыз және қосалқы Басқару сервері басқаратын виртуалды Басқару серверіне қосыла алмасаңыз, келесі тәсілдердің бірін пайдалана аласыз:

- **Сенімді Басқару серверлері тізіміне қосалқы Серверді қосу арқылы қолданыстағы Kaspersky Security Center Web Console орнатуын өзгертіңіз**. Осыдан кейін, сіз виртуалды Басқару серверіне Kaspersky Security Center Web Console веб-консоліне қосыла аласыз.

  1. Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыда ksc-web-console-<нұсқа нөмірі>.<жинақ нөмірі>.exe орындалатын файлын әкімші құқықтары бар есептік жазбамен іске қосыңыз.

     Бағдарламаны орнату шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

  2. **Жаңарту** параметрін таңдаңыз.

  3. **Өзгеріс түрі** бетінде **Қосылым параметрлерін өзгерту** параметрін таңдаңыз.

  4. **Сенімді Басқару серверлері** қадамында қажетті қосалқы Басқару серверлерін қосыңыз.

  5. Соңғы қадамда, жаңа параметрлерді қолдану үшін **Өзгерту** түймесін басыңыз.

  6. Бағдарламаны орнату сәтті аяқталғаннан кейін **Дайын** түймесін басыңыз.

- Виртуалды Сервер құрылған қосалқы Басқару серверіне тікелей қосылу үшін Kaspersky Security Center Web Console пайдаланыңыз. Осыдан кейін, сіз Kaspersky Security Center Web Console веб-консолінде виртуалды Басқару серверіне ауыса аласыз.

- Виртуалды Серверге тікелей қосылу үшін MMC негізіндегі Басқару консолін пайдаланыңыз.

Басқару серверлерінің иерархиясын жою

Егер сізге бұдан былай Басқару сервері иерархиясы қажет болмаса, оларды осы иерархиядан ажыратуға болады.

Басқару сервері иерархиясын жою үшін:

1. Басты мәзірде негізгі Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.

3. Қосалқы Басқару серверін жойғыңыз келетін басқару тобында қосалқы Басқару серверін таңдаңыз.

4. Мәзірден **Жою** тармағын таңдаңыз.

5. Ашылған терезеде қосалқы Басқару серверін жоюды растау үшін **ОК** түймесін басыңыз.

Бұрынғы негізгі Басқару сервері және бұрынғы қосалқы Басқару сервері енді бір-бірінен тәуелсіз. Серверлер иерархиясы енді жоқ.

Басқару серверіне техникалық қызмет көрсету

Басқару серверіне техникалық қызмет көрсету, Басқару сервері қалтасында орынды босатуға және қажет емес нысандарды жою арқылы дерекқордың өлшемін азайтуға мүмкіндік береді. Бұл қолданбаның өнімділігі мен сенімділігін жақсартуға көмектеседі. Басқару серверіне аптасына бір реттен сиретпей техникалық қызмет көрсету ұсынылады.

Басқару серверіне техникалық қызмет көрсету тиісті тапсырманың көмегімен орындалады. Басқару серверіне техникалық қызмет көрсету барысында бағдарлама келесі әрекеттерді орындайды:

- Сақтау қалтасынан қажет емес қалталар мен файлдарды жояды.

- Кестелерден қажет емес жазбаларды жояды («аспалы көрсеткіштер» деп те аталады).

- Кэшті тазартады.

- Дерекқорға қызмет көрсетеді (егер сіз SQL Server немесе PostgreSQL ДҚБЖ ретінде пайдалансаңыз):

  - дерекқорды қателер тұрғысынан тексереді (тек SQL Server үшін қолжетімді);

  - дерекқордың индекстерін қайта құрады;

  - дерекқордың статистикасын жаңартады;

  - дерекқорды қысады (қажет болса).

Басқару серверіне техникалық қызмет көрсету тапсырмасы Kaspersky Security Center орнату кезінде автоматты түрде жасалады. Басқару серверіне техникалық қызмет көрсету тапсырмасы жойылған, сіз оны қолмен жасай аласыз.

Басқару серверіне техникалық қызмет көрсету тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. Шебердің **Жаңа тапсырма параметрлері** терезесінде **Басқару серверіне техникалық қызмет көрсету** тапсырма түрін таңдап, **Келесі** түймесін басыңыз.
4. Шебердің келесі қадамдарын орындаңыз.

Нәтижесінде, жасалған тапсырма тапсырмалар тізімінде көрсетіледі. Бір Басқару сервері үшін бір Басқару серверіне техникалық қызмет көрсету тапсырмасы ғана орындалуы мүмкін. Басқару серверіне техникалық қызмет көрсету тапсырмасы Басқару сервері үшін әлдеқашан жасалған болса, басқа Басқару серверіне техникалық қызмет көрсету тапсырмасын жасау мүмкін емес.

Интерфейсті конфигурациялау

Сіз Kaspersky Security Center Web Console интерфейсін пайдаланылатын функцияларға байланысты интерфейс бөлімдері мен элементтерін көрсетуге және жасыруға конфигурациялай аласыз.

Kaspersky Security Center Web Console интерфейсін қазіргі уақытта қолданылатын функциялар жиынтығына сай конфигурациялау үшін:

1. Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Интерфейс опциялары** тармағын таңдаңыз.
2. Пайда болған **Интерфейс опциялары** терезесінде қажетті параметрлерді қосыңыз немесе өшіріңіз.
3. **Сақтау** түймесін басыңыз.

Содан соң, консольде қосулы параметрлерге сәйкес басты мәзірдегі бөлімдер көрсетіледі. Мысалы, **EDR ескертулерін көрсету** қоссаңыз, **Бақылау және есеп беру** → **Ескертулер** бөлімі басты мәзірде пайда болады.

Виртуалды Басқару серверлерін басқару

Бұл бөлімде виртуалды Басқару серверлерін қалай басқаруға болатындығы сипатталған:

- Виртуалды Басқару серверлерін жасау
- Виртуалды Басқару серверлерін қосу және өшіру
- Виртуалды Басқару сервері әкімшісін тағайындау

- Клиент құрылғылары үшін Басқару серверін ауыстыру
- Виртуалды Басқару серверлерін жою

Виртуалды Басқару серверін жасау

Виртуалды Басқару серверлерін жасауға және оларды басқару топтарына қосуға болады.

Виртуалды Басқару серверін құру кезінде, ол пайдаланушылар тізімін және негізгі Басқару серверінің барлық пайдаланушы құқықтарын иеленеді. Егер пайдаланушының басты Серверге қатынасу құқығы болса, онда бұл пайдаланушының виртуалды Серверге қатынасу құқығы да бар. Жасалғаннан кейін, серверлерге қол жеткізу құқықтарын өзіңіз конфигурациялайсыз.

Виртуалды Басқару серверін жасау және қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.
2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.
3. Виртуалды Басқару серверін қосқыңыз келетін басқару тобын таңдаңыз.
   Виртуалды Басқару сервері құрылғыларды таңдалған топтан (оның ішінде ішкі топтардан) басқарады.
4. Мәзірден **Жаңа виртуалды Басқару сервері** тармағын таңдаңыз.
5. Ашылған бетте жаңа виртуалды Басқару серверінің сипаттарын белгілеңіз:
   - **Виртуалды Басқару серверінің атауы**.
   - **Басқару серверінің қосылу мекенжайы**
     Басқару серверінің атын немесе IP мекенжайын көрсетуге болады.
6. Пайдаланушылар тізімінен виртуалды Басқару сервері әкімшісін таңдаңыз. Қажет болса, қолданыстағы есептік жазбаны әкімші рөлін тағайындамас бұрын өзгертуге болады; жаңа есептік жазба да жасалуы мүмкін.
7. **Сақтау** түймесін басыңыз.

   Жаңа виртуалды Басқару сервері жасалды, басқару тобына қосылды және **Басқару серверлері** қойыншасында көрсетіледі.

Егер сіз Kaspersky Security Center Web Console веб-консолиндегі негізгі Басқару серверіне қосылған болсаңыз және қосалқы Басқару сервері басқаратын виртуалды Басқару серверіне қосыла алмасаңыз, келесі тәсілдердің бірін пайдалана аласыз:

- **Сенімді Басқару серверлері тізіміне қосалқы Серверді қосу арқылы қолданыстағы Kaspersky Security Center Web Console орнатуын өзгертіңіз**. Осыдан кейін, сіз виртуалды Басқару серверіне Kaspersky Security Center Web Console веб-консолінe қосыла аласыз.

  1. Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыда ksc-web-console-<нұсқа нөмірі>.<жинақ нөмірі>.exe орындалатын файлын әкімші құқықтары бар есептік жазбамен іске қосыңыз.

     Бағдарламаны орнату шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Жаңарту** параметрін таңдаңыз.

3. **Өзгеріс түрі** бетінде **Қосылым параметрлерін өзгерту** параметрін таңдаңыз.

4. **Сенімді Басқару серверлері** қадамында қажетті қосалқы Басқару серверлерін қосыңыз.

5. Соңғы қадамда, жаңа параметрлерді қолдану үшін **Өзгерту** түймесін басыңыз.

6. Бағдарламаны орнату сәтті аяқталғаннан кейін **Дайын** түймесін басыңыз.

- Виртуалды Сервер құрылған қосалқы Басқару серверіне тікелей қосылу үшін Kaspersky Security Center Web Console пайдаланыңыз. Осыдан кейін, сіз Kaspersky Security Center Web Console веб-консолінде виртуалды Басқару серверіне ауыса аласыз.

- Виртуалды Серверге тікелей қосылу үшін MMC негізіндегі Басқару консолін пайдаланыңыз.

Виртуалды Басқару серверін қосу және өшіру

Виртуалды Басқару серверін жасаған кезде, ол әдепкі бойынша қосылады. Оны кез келген уақытта өшіруге немесе қайта қосуға болады. Виртуалды Басқару серверін өшіру немесе қосу физикалық Басқару серверін өшіруге немесе қосуға тең.

Виртуалды Басқару серверін қосу немесе өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.

3. Қосқыңыз немесе өшіргіңіз келетін виртуалды Басқару серверін таңдаңыз.

4. Мәзірде **Виртуалды Басқару серверін қосу / өшіру** түймесін басыңыз.

Виртуалды Басқару серверінің күйі оның алдыңғы күйіне байланысты қосулы немесе өшірулі болып өзгереді. Жаңартылған күй Басқару сервері атауының жанында көрсетіледі.

Виртуалды Басқару сервері әкімшісін тағайындау

Ұйымыңызда виртуалды Басқару серверлерін пайдалансаңыз, әрбір виртуалды Басқару сервері үшін бөлек әкімші тағайындау қажет болуы мүмкін. Мысалы, бұл сіздің ұйымыңыздың жеке кеңселерін немесе бөлімдерін басқару үшін виртуалды Басқару серверлерін құрған кезде немесе сіз провайдер (MSP) болсаңыз және виртуалды Басқару серверлері арқылы клиенттеріңізді басқарсаңыз пайдалы болуы мүмкін.

Виртуалды Басқару серверін құру кезінде, ол пайдаланушылар тізімін және негізгі Басқару серверінің барлық пайдаланушы құқықтарын иеленеді. Егер пайдаланушының басты Серверге қатынасу құқығы болса, онда бұл пайдаланушының виртуалды Серверге қатынасу құқығы да бар. Жасалғаннан кейін, сіз Серверлерге қатынасу құқығын өзіңіз конфигурациялайсыз. Егер сіз тек виртуалды Басқару серверіне әкімші тағайындағыңыз келсе, әкімшінің негізгі Басқару серверінде қатынасу құқығы жоқ екеніне көз жеткізіңіз.

Сіз виртуалды Басқару серверіне әкімші рұқсаттарын беру арқылы виртуалды Басқару сервері әкімшісін тағайындайсыз. Сіз келесі жолдардың бірімен қажетті қатынасу құқықтарын бере аласыз:

- Әкімші үшін қатынасу құқықтарын қолмен конфигурациялаңыз.
- Әкімшіге бір немесе бірнеше пайдаланушы рөлдерін тағайындаңыз.

Kaspersky Security Center Web Console серверіне кіру үшін виртуалды Басқару серверінің әкімшісі виртуалды Басқару серверінің атауын, пайдаланушы атын және құпиясөзді көрсетеді. Kaspersky Security Center Web Console сервері әкімшінің түпнұсқалық растамасын орындайды және әкімшінің қатынасу құқығы бар виртуалды Басқару серверін ашады. Әкімші Басқару серверлері арасында ауыса алмайды.

Алдын ала талаптар

Келесі шарттардың орындалғанына көз жеткізіңіз:

- Виртуалды Басқару сервері жасалды.
- Негізгі Басқару серверінде, сізде виртуалды Басқару серверіне тағайындағыңыз келетін әкімші үшін есептік жазба жасалған.
- Сізде **Жалпы функционал** → **Пайдаланушы рұқсаттары** функционалдық аймағында **Нысан ACL параметрлерін өзгерту** құқығыңыз бар.

Қатынасу құқықтарын қолмен конфигурациялау

Виртуалды Басқару сервері әкімшісін тағайындау үшін:

1. Бас мәзірден қажетті виртуалды Басқару серверіне ауысыңыз:
   a. Басқару серверінің ағымдағы атауының оң жағындағы шеврон (›) белгішесін басыңыз.
   b. Қажетті Басқару серверін таңдаңыз.
2. Басты мәзірде Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.
   Басқару серверінің сипаттары терезесі ашылады.
3. **Қатынасу құқықтары** қойыншасында **Қосу** түймесін басыңыз.
   Негізгі Басқару сервері мен ағымдағы виртуалды Басқару сервері пайдаланушыларының бірыңғай тізімі ашылады.
4. Пайдаланушылар тізімінен виртуалды Басқару серверіне тағайындағыңыз келетін әкімші есептік жазбасын таңдап, **OK** түймесін басыңыз.
   Бағдарлама таңдалған пайдаланушыны пайдаланушылар тізіміне, **Қатынасу құқықтары** қойыншасына қосады.
5. Қосылған есептік жазбаның жанына жалаушаны қойып, **Қатынасу құқықтары** түймесін басыңыз.
6. Виртуалды Басқару серверінде әкімші құқықтарын конфигурациялаңыз.

Сәтті түпнұсқалық растамаүшін әкімшінің келесі құқықтары болуы керек:

- **Оқу** → **Жалпы функционал** функционалдық аймағындағы **Базалық функционалдылық** құқығы.
- **Оқу** → **Жалпы функционал** функционалдық аймағындағы **Виртуалды Басқару серверлері** құқығы.

Бағдарлама өзгертілген пайдаланушы құқықтарын әкімші есептік жазбасында сақтайды.

Пайдаланушы рөлдерін тағайындау арқылы қатынасу құқығын конфигурациялау

Сондай-ақ, сіз виртуалды Басқару сервері әкімшісіне пайдаланушы рөлі арқылы қатынасу құқығын бере аласыз. Мысалы, егер сіз бір виртуалды Басқару серверіне бірнеше әкімші тағайындағыңыз келсе, бұл пайдалы болуы мүмкін. Бұл жағдайда, сіз бірнеше әкімші үшін бірдей құқықтарды конфигурациялаудың орнына әкімші есептік жазбаларына бір немесе бірнеше пайдаланушы рөлдерін тағайындай аласыз.

Виртуалды Басқару сервері әкімшісін тағайындау мақсатында оған пайдаланушы рөлдерін тағайындау үшін:

1. Негізгі Басқару серверінде пайдаланушы рөлін жасаңыз және виртуалды Басқару серверінде әкімші ие болуы тиісті барлық қажетті қатынасу құқықтарын көрсетіңіз. Сіз бірнеше рөлдерді жасай аласыз, мысалы, әртүрлі функционалды аймақтарға қатынасуды бөлгіңіз келсе.
2. Бас мәзірден қажетті виртуалды Басқару серверіне ауысыңыз:
   a. Басқару серверінің ағымдағы атауының оң жағындағы шеврон (›) белгішесін басыңыз.
   b. Қажетті Басқару серверін таңдаңыз.
3. Әкімші есептік жазбаның жаңа рөлін немесе бірнеше рөлдерін тағайындаңыз.

Бағдарлама әкімші есептік жазбасының рөлін тағайындайды.

Нысан деңгейінде қатынасу құқықтарын конфигурациялау

Функционалды аймақ деңгейінде қатынасу құқықтарын тағайындаудан басқа, сіз виртуалды Басқару серверіндегі белгілі бір нысандарға, мысалы, белгілі бір басқару тобына немесе тапсырмаға қатынасуды конфигурациялай аласыз. Ол үшін, виртуалды Басқару серверіне ауысыңыз, содан кейін нысан сипаттарындағы қатынасу құқықтарын конфигурациялаңыз.

Клиент құрылғылары үшін Басқару серверін ауыстыру

Басқару серверін ауыстыру тапсырмасы көмегімен клиент құрылғыларын басқаратын басқару серверін басқа серверге ауыстыруға болады. Тапсырма аяқталғаннан кейін, таңдалған клиент құрылғылары көрсетілген Басқару серверінің басқаруында болады.

> Басқару серверіне қосылым шлюздері арқылы қосылған клиент құрылғыларында *Басқару серверін ауыстыру* тапсырмасын пайдалану мүмкін емес. Мұндай құрылғылар үшін Желілік агентті қайта конфигурациялау немесе желілік агентті қайта орнату және қосылым шлюзін көрсету керек.

Клиент құрылғылары жұмыс істейтін Басқару серверін басқа Сервермен ауыстыру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Шебердің **Жаңа тапсырма параметрлері** қадамында келесі параметрлерді көрсетіңіз:

   a. **Бағдарлама** ашылмалы тізімінде **Kaspersky Security Center** опциясын таңдаңыз.

   b. **Тапсырма түрі** өрісінде **Басқару серверін ауыстыру** опциясын таңдаңыз.

   c. **Тапсырманың атауы** өрісінде жасап жатқан тапсырма атауын көрсетіңіз.

      Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

   d. Тапсырма тағайындалатын құрылғыларды таңдаңыз.

      - **Басқару тобына тапсырманы белгілеу**

        Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

        Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

        Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

      - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

        Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

        Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

      - **Құрылғы таңдауына тапсырманы белгілеу**

        Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

        Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

4. Шебердің **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғы таңдауын көрсетіңіз.

5. Шебердің келесі қадамында клиент құрылғыларына арналған басқару серверін өзгерту шарттарына келісетініңізді растаңыз.

6. Шебердің келесі қадамында таңдалған құрылғыларды басқару үшін қолданғыңыз келетін басқару серверін таңдаңыз:

   - **Басқа негізгі Басқару серверіне өзгертіңіз**

     Клиент құрылғыларын басқа негізгі басқару серверіне жылжыту үшін келесі басқару серверінің қосылым параметрлерін көрсетіңіз:

     1. **Басқару серверінің мекенжайы** өрісінде жаңа негізгі басқару серверінің мекенжайын көрсетіңіз.
     2. **Порт нөмірі** өрісінде басқару серверіне қосылу үшін порт нөмірін көрсетіңіз.

        Әдепкі бойынша 14000-порт орнатылған.
     3. **SSL порты** өрісінде негізгі басқару серверінің SSL портының нөмірін көрсетіңіз.

        Әдепкі бойынша 13000-порт орнатылған.
     4. Қажет болса, **Прокси-серверді пайдалану** опциясын қосыңыз.

        Бұл опция өшірілсе, құрылғыны басқару серверіне қосу үшін тікелей қосылым қолданылады.

        Бұл параметр қосылса, прокси сервер параметрлерін көрсетіңіз:

        - **Прокси-сервердің мекенжайы**
        - **Прокси-сервердің порты**

        Прокси-серверге аутентификация қажет болса, прокси-сервер қосылымы орнатылатын есептік жазбаның **Пайдаланушы аты** және **Құпиясөз** өрістерінде есептік жазбаның кіру деректерін көрсетіңіз. Прокси-сервердегі түпнұсқалық растама үшін ғана талап етілетін ең аз құқықтарға ие есептік жазба деректерін беру ұсынылады.
     5. Қажет болса, жаңа басқару сервері сертификатын жүктеп салыңыз.

   - **Осы негізгі сервердегі басқа виртуалды Басқару серверіне өзгертіңіз**

     Клиент құрылғыларын ағымдағы негізгі басқару серверіндегі виртуалды басқару серверіне жылжыту үшін осы опцияны таңдаңыз. Ол үшін **Виртуалды Басқару серверінің атауы** ашылмалы тізімінде қажетті виртуалды басқару серверін таңдаңыз.

7. Шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында есептік жазба параметрлерін көрсетіңіз:

   - **Әдепкі есептік жазба**

     Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Есептік жазбаны көрсету**

     Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

     - **Есептік жазба**

       Тапсырманы іске қосатын есептік жазба.

- **Құпиясөз**

  Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

8. Әдепкі тапсырма параметрлерін өзгерткіңіз келсе, шебердің **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** опциясын қосыңыз.

   Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі параметрлерді кез келген уақытта өзгертуге болады.

9. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

10. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

11. Әдепкі тапсырма параметрлерін өзгерткіңіз келсе, тапсырма сипаттары терезесінде қажеттіліктеріңізге сәйкес жалпы тапсырма параметрлерін көрсетіңіз.

12. **Сақтау** түймесін басыңыз.

    Тапсырма жасалды және конфигурацияланды.

13. Жасалған тапсырманы іске қосыңыз.

Тапсырма аяқталғаннан кейін, ол жасалған клиент құрылғылары тапсырма параметрлерінде көрсетілген басқару серверінің басқаруына өтеді.

Виртуалды Басқару серверін жою

Виртуалды Басқару сервері жойылған кезде, Басқару серверінде жасалған барлық нысандар, соның ішінде саясаттар мен тапсырмалар да жойылады. Виртуалды Басқару сервері басқарған басқару топтарынан басқарылатын құрылғылар басқару топтарынан жойылады. Құрылғыларды Kaspersky Security Center басқаруына қайтару үшін желі сауалнамасын орындаңыз, содан кейін табылған құрылғыларды Тағайындалмаған құрылғылар тобынан басқару топтарына жылжытыңыз.

Виртуалды Басқару серверін жою үшін:

1. Басты мәзірде Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

2. Ашылған бетте **Басқару серверлері** қойыншасына өтіңіз.

3. Жойғыңыз келетін виртуалды Басқару серверін таңдаңыз.

4. Мәзірде **Жою** түймесін басыңыз.

Виртуалды Басқару сервері жойылды.

Есептік жазбаны рұқсатсыз өзгертуден қорғауды қосу

Сондай-ақ, сіз пайдаланушының есептік жазбасын рұқсатсыз өзгертуден қорғауды да қоса аласыз. Бұл параметр қосулы болса, пайдаланушының есептік жазбасының параметрлерін өзгерту үшін, өзгерту құқықтары бар пайдаланушы авторизациядан өтуі қажет.

Есептік жазбаны рұқсатсыз өзгертуден қорғауды қосу немесе өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар** бөліміне өтіңіз.
2. Есептік жазбаны рұқсатсыз өзгертуден қорғауды конфигурациялағыңыз келетін ішкі пайдаланушы есептік жазбасын басыңыз.
3. Ашылған пайдаланушы сипаттары терезесінде **Есептік жазба қорғанысы** қойыншасын таңдаңыз.
4. Есептік жазба параметрлерін өзгерткен кезде есептік деректерді әрбір рет сұрағыңыз келсе, **Есептік жазба қорғанысы** қойыншасында **Пайдаланушылардың есептік жазбаларын өзгертуге берілген рұқсатты тексеру үшін түпнұсқалық растаманы сұрау** параметрін таңдаңыз. Не болмаса, **Пайдаланушыларға осы есептік жазбаны қосымша түпнұсқалық растамасыз өзгертуге рұқсат беру** нұсқасын таңдаңыз.
5. **Сақтау** түймесін басыңыз.

Пайдаланушы есептік жазбасы үшін рұқсатсыз өзгертуден қорғау қосылған.

Басқару сервері деректерін сақтық көшірмелеу және қалпына келтіру

Деректердің сақтық көшірмесі Басқару серверін бір құрылғыдан екіншісіне ақпаратты жоғалтпай тасымалдауға мүмкіндік береді. Сақтық көшірме жасау арқылы басқару сервері дерекқорын басқа құрылғыға жылжытқанда немесе Kaspersky Security Center бағдарламасының жаңа нұсқасына жаңартқанда деректерді қалпына келтіре аласыз. Сонымен қатар Басқару сервері деректерін Kaspersky Security Center Linux басқаруындағы Kaspersky Security Center Windows жүйесінен жылжыту үшін деректердің сақтық көшірмесін пайдалануға болады (деректерді Kaspersky Security Center Linux жүйесінен Kaspersky Security Center Windows жүйесіне жылжытуға қолдау көрсетілмейді).

Орнатылған басқару плагиндерінің сақтық көшірмелері сақталмайтынын ескеріңіз. Сақтық көшірмеден Басқару сервері деректерін қалпына келтіргеннен кейін, басқарылатын бағдарлама плагиндерін жүктеп, қайта орнату қажет.

Басқару сервер деректерінің сақтық көшірмесін жасамас бұрын, басқару тобына виртуалды Басқару серверінің қосылғанын тексеріңіз. Сақтық көшірме жасау алдында виртуалды Басқару сервер қосылса, осы виртуалды серверге әкімші тағайындалғанын тексеріңіз. Сақтық көшірмеден кейін виртуалды Басқару серверге әкімші құқықтарын бере алмайсыз. Әкімшінің тіркелгі деректері жоғалса, виртуалды әкімші серверіне жаңа әкімші тағайындай алмайтыныңызды ескеріңіз.

Kaspersky Security Center ақауларға төзімді кластерінің сақтық көшірмесін жасау немесе қалпына келтіру үшін бүкіл кластерді техникалық қызмет көрсету үшін тоқтатып, сақтық көшірме жасау немесе қалпына келтіру аяқталғаннан кейін оны қайта іске қосу керек.

Басқару сервері деректерінің сақтық көшірмесін келесі тәсілдердің бірімен жасауға болады:

- Басқару консолі арқылы деректерді сақтық көшірмелеу тапсырмасын жасау және іске қосу.
- Басқару сервері орнатылған құрылғыда klbackup утилитасын іске қосу. Утилита Kaspersky Security Center жеткізу жиынтығының құрамына кіреді. Басқару серверін орнатқаннан кейін, утилита бағдарламаны орнату кезінде көрсетілген мақсатты қалтаның түбірінде болады.

Басқару сервері деректерінің сақтық көшірмесінде келесі деректер сақталады:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері).
- Басқару топтары құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат.
- Қашықтан орнатуға арналған бағдарлама дистрибутивтері қоймасы.
- Басқару сервері сертификаты.
- *Жаңартулар* қалтасының мазмұны.

  Әдепкісінше қалта жолы — C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Басқару сервері деректерін тек klbackup утилитасының көмегімен қалпына келтіруге болады. Жаңа ғана орнатылған және сақтық көшірме жасалған нұсқамен бірдей (немесе одан кейінгі) басқару серверінің жұмыс істейтін данасында ғана қалпына келтіруге болады.

Деректерді сақтық көшірмелеу тапсырмасын жасау

Сақтық көшірмелеу тапсырмасы Басқару серверінің тапсырмасы болып табылады және оны бағдарламаны жылдам іске қосу шебері жасайды. Бағдарламаны жылдам іске қосу шебері жасаған сақтық көшірмелеу тапсырмасы жойылса, оны қолмен жасауға болады.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. Шебердің **Жаңа тапсырма параметрлері** терезесінде **Басқару сервері деректерінің резервтік қоймасы** тапсырма түрін таңдаңыз.
4. Шебердің келесі қадамдарын орындаңыз.

Басқару сервері деректерінің резервтік қоймасы тапсырмасын тек бір данада жасауға болады. Басқару сервері деректерін сақтық көшірмелеу тапсырмасы Басқару сервері үшін жасалған болса, онда ол сақтық көшірмелеу тапсырмасын жасау шеберінің тапсырма түрін таңдау терезесінде көрсетілмейді.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіп, **Басқару сервері деректерінің резервтік қоймасы** тапсырмасын таңдаңыз.

2. **Басқару сервері деректерінің резервтік қоймасы** тапсырмасының атауын басыңыз.

   Тапсырма сипаттары терезесі ашылады.

3. Қажет болса, өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіңіз.

4. **Бағдарлама параметрлері** бөлімінде Басқару сервері деректерінің сақтық көшірмелерін сақтауға арналған қалтаға апаратын жолды көрсетіңіз, сақтық көшірме құпиясөзінің қорғанысын және қажет болса, сақтық көшірмелердің санын орнатыңыз.

5. Өзгерістерді қолдану үшін **Сақтау** түймесін басыңыз.

Басқару сервері деректерін сақтық көшірмелеу тапсырмасы конфигурацияланған.

Басқару серверін басқа құрылғыға тасымалдау

Егер сізге жаңа құрылғыда Басқару серверін пайдалану қажет болса, оны келесі тәсілдердің бірімен тасымалдауға болады:

- Басқару серверін және дерекқор серверін жаңа құрылғыға жылжытыңыз (дерекқор серверін жаңа құрылғыға басқару серверімен бірге немесе басқа құрылғыға орнатуға болады).

- Дерекқор серверін ескі құрылғыда қалдыру және жаңа құрылғыға тек Басқару серверін тасымалдау.

Басқару серверін мен дерекқор серверін жаңа құрылғыға жылжыту үшін:

1. Алдыңғы құрылғыда Басқару сервері деректерінің сақтық көшірмесін жасаңыз.

   Бұл үшін, Kaspersky Security Center Web Console көмегімен деректерді сақтық көшірмелеу тапсырмасын іске қосыңыз немесе klbackup утилитасын іске қосыңыз.

   > Егер сіз SQL Server серверін Басқару сервері үшін ДҚБЖ ретінде қолдансаңыз, деректерді SQL Server серверінен MySQL немесе MariaDB ДҚБЖ жүйесіне тасымалдауға болады. Деректерді сақтық көшірмелеу үшін klbackup утилитасын интерактивті режимде іске қосыңыз. Сақтық көшірмелеу және деректерді қалпына келтіру шеберінің **Сақтық көшірмелеу параметрлері** терезесінде **MySQL/MariaDB пішіміне көшіру** параметрін қосыңыз. Kaspersky Security Center бағдарламасы MySQL және MariaDB серверімен үйлесімді деректердің сақтық көшірмесін жасайды. Осыдан кейін, сіз деректерді MySQL немесе MariaDB серверіндегі сақтық көшірмесінен қалпына келтіре аласыз.

   > Сондай-ақ, деректерді SQL Server серверінен Azure SQL ДҚБЖ жүйесіне тасымалдағыңыз келсе, **Azure пішіміне ауысу** параметрін қосуға болады.

2. Алдыңғы құрылғыда басқару серверін желіден ажыратыңыз.

3. Басқару сервері орнатылатын жаңа құрылғыны таңдаңыз. Таңдалған құрылғыдағы аппараттық және бағдарламалық жасақтама Басқару серверіне, Kaspersky Security Center Web Console серверіне және Желілік агентке қойылатын талаптарға сәйкес келетініне көз жеткізіңіз. Басқару серверінде қолданылатын порттардың қолжетімді екеніне көз жеткізіңіз.

4. Жаңа құрылғыға сол мекенжайды тағайындаңыз.

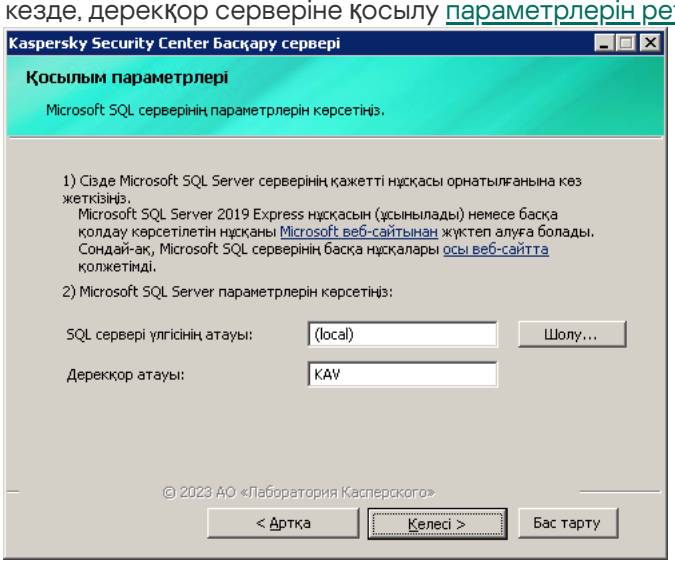
   Жаңа басқару серверіне NetBIOS атауын, FQDN және статикалық IP мекенжайын тағайындауға болады. Бұл желілік агенттер орналастырылған кезде желілік агенттің орнату бумасында басқару серверінің қандай мекенжайы орнатылғанына байланысты. Сондай-ақ желілік агент қосылатын басқару серверін анықтайтын қосылым мекенжайын пайдалануға болады (бұл мекенжайды klnagchk қызметтік бағдарламасын қолданып, басқарылатын құрылғыларда алуға болады).

5. Қажет болса, жаңа құрылғыда басқару сервері пайдаланатын дерекқорларды басқару жүйесін (ДҚБЖ) орнатыңыз.

   Дерекқорды басқару серверімен бірге жаңа құрылғыға немесе басқа құрылғыға орнатуға болады. Таңдалған құрылғы аппараттық және бағдарламалық талаптарға сәйкес келетініне көз жеткізіңіз. ДҚБЖ таңдау кезінде Басқару сервері қызмет көрсететін құрылғылардың санын ескеріңіз.

6. Жаңа құрылғыда басқару серверінің орнатылымын іске қосыңыз.

7. Басқару серверін орнатқан кезде, дерекқор серверіне қосылу параметрлерін реттеңіз.



Microsoft SQL Server үшін қосылым параметрлері терезесінің мысалы

Дерекқор серверін қайда орналастыру керек екеніне байланысты, келесі әрекеттердің бірін орындаңыз:

- **Алдыңғы құрылғыда дерекқор серверін қалдырыңыз.**

  1. **SQL сервері үлгісінің атауы** өрісінің жанында **Шолу** түймесін басыңыз және пайда болған тізімде алдыңғы құрылғының атауын таңдаңыз.

     Алдыңғы құрылғы жаңа Басқару серверімен байланысу үшін қолжетімді болуы керек екенін ескеріңіз.

  2. **Дерекқор атауы** өрісінде алдыңғы дерекқор атауын енгізіңіз.

- **Дерекқор серверін басқа құрылғыға жылжытыңыз.**

  1. **SQL сервері үлгісінің атауы** өрісінің жанында **Шолу** түймесін басыңыз және пайда болған тізімде құрылғы атауын таңдаңыз.

  2. **Дерекқор атауы** өрісінде жаңа дерекқор атауын енгізіңіз.

     Жаңа дерекқордың атауы алдыңғы құрылғыдағы дерекқордың атауына сәйкес келуі керек екенін ескеріңіз. Басқару серверінің сақтық көшірмесін пайдалану үшін дерекқорлардың атауы сәйкес келуі керек. Дерекқордың әдепкі бойынша атауы *KAV*.

8. Орнату аяқталғаннан кейін, klbackup утилитасын көмегімен жаңа құрылғыдағы Басқару сервері деректерін қалпына келтіріңіз.

   Егер сіз SQL Server серверін алдыңғы және жаңа құрылғыларда ДҚБЖ ретінде қолдансаңыз, жаңа құрылғыда орнатылған SQL Server нұсқасы алдыңғы құрылғыда орнатылған SQL Server нұсқасымен бірдей немесе одан жоғары болуы керек екенін ескеріңіз. Әйтпесе, сіз жаңа құрылғыдағы Басқару сервері деректерін қалпына келтіре алмайсыз.

9. Kaspersky Security Center Web Console бағдарламасын ашып, Басқару серверіне қосылыңыз.

10. Барлық басқарылатын құрылғылар басқару серверіне қосылғанына көз жеткізіңіз.

11. Алдыңғы құрылғыдан Басқару сервері мен дерекқорлар серверін жойыңыз.

Басқару консолін Басқару сервері мен дерекқор серверін басқа құрылғыға тасымалдау үшін де пайдалануға болады.

klscmodchk және integrity_checker утилиталарын пайдалану арқылы модульдердің тұтастығын тексеру

Kaspersky Security Center Linux құрамында динамикалық түрде байланысқан кітапханалар, орындалатын файлдар, конфигурация файлдары және интерфейс файлдары түріндегі бірнеше екілік модуль бар. Зиянкестер бір немесе бірнеше орындалатын модульді немесе қолданба файлдарын зиянды кодты қамтитын басқа файлдармен ауыстыруы мүмкін. Модуль мен файлдарды ауыстыруға жол бермеу үшін Kaspersky Security Center Linux жүйесі klscmodchk және integrity_checker утилиталарын пайдалану арқылы құрамдас тұтастығының тексерісін қамтамасыз етеді. Бұл утилиталар модульдер мен файлдарда рұқсат етілмеген өзгерістер мен зақымның бар-жоғын тексереді. Модульде немесе қолданба файлында қате тексеру сомасы болса, ол зақымдалған болып саналады.

Klscmodchk утилитасы келесі Kaspersky Security Center құрамдастарының тұтастығын тексереді:

- Басқару сервері
- Желілік агент
- Манифест файлдары бар басқару консоліне арналған басқару плагиндері

Integrity_checker утилитасы келесі Kaspersky Security Center құрамдастарының тұтастығын тексереді:

- Басқару сервері
- Желілік агент
- Kaspersky Security Center Web Console

Екі утилита да Kaspersky Security Center құрылымының бір бөлігі болатын және орнату қалтасында орналасқан kl_file_integrity_manifest.xml манифест файлының негізінде модуль тұтастығын тексереді. Құрамдастың манифест файлында тұтастығы Kaspersky Security Center құрамдасының дұрыс жұмыс істеуі үшін маңызды файлдар бар. Манифест файлдарының тұтастығы да тексеріледі.

Kl_file_integrity_manifest.xml манифест файлын өзгерту ұсынылмайды, себебі бұл сандық қолтаңбаны жарамсыз қылады және тұтастықты тексеру сәтсіз аяқталады.

Kaspersky Security Center құрамдасының тұтастығын тексеру үшін келесі пәрмендердің бірін орындаңыз:

- `$ klscmodchk [ параметрлер ]`

  Klscmodchk утилитасы integrity_checker утилитасын `--verbose` параметрімен іске қосады және модульдердің тұтастығын тексереді.

  Klscmodchk утилитасының параметрлері:

  - `-logfile <log_file_path>`: журналға жазу үшін дискідегі файл жолын көрсетіңіз. Әдепкісінше ақпарат консольге шығарылады.
  - `-chkplugins`: манифест файлдары бар басқару консоліне арналған орнатылған басқару плагині модульдерінің тұтастығын тексеру. Әдепкісінше басқару плагиндері тексерілмейді.
  - `-verbose`: тұтастықты тексеру кезінде кеңейтілген ақпаратты шығару.

- `$ integrity_checker [ параметрлер ] <манифест_файлының_жолы>`

  Integrity_checker утилитасының параметрлері:

  - `--help`: integrity_checker утилитасының анықтамасын көрсету.
  - `--version`: integrity_checker утилитасының нұсқасын көрсету.
  - `--verbose`: утилитаның жұмысы туралы ақпаратты көрсету. Тұтастығын тексеру кезінде пәрменде осы параметрді пайдалану жеткілікті.

Әрбір манифест файлын тексеру нәтижесі манифест файлы атауының жанында келесі форматта көрсетіледі:

- SUCCEEDED: файлдың тұтастығы расталды (қайтару коды: 0).
- FAILED: файлдың тұтастығы расталмады (нөлге тең емес емес қайтару коды).

Сондай-ақ қолданбаны іске қосқан кезде автоматты түрде іске қосылуы үшін, тұтастық тексерістерін конфигурациялауға болады. Тұтастықты автоматты түрде тексеру әдепкісінше өшірілген болады.

Тұтастықты автоматты түрде тексеруді қосу үшін:

1. Басқару сервері орнатылған құрылғыда Windows пәрмен жолына келесі пәрменді енгізіңіз:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Құрылғыны өшіріп қосыңыз.

Тұтастықты автоматты түрде тексеру қосылды.

Kaspersky Security Center келесіде іске қосылғанда, klscmodchk утилитасы басқару серверімен бірге іске қосылады және модульдердің тұтастығын тексеруді бастайды. Тұтастықты тексеру нәтижесі Kaspersky Event журналына жазылады.

Kaspersky Security Center Web Console бастапқы конфигурациялау

Бұл бөлімде бастапқы конфигурациялау үшін Kaspersky Security Center Web Console орнатқаннан кейін орындалатын қадамдар сипатталған.

Бағдарламаны жылдам іске қосу шебері (Kaspersky Security Center Web Console)

Бұл бөлімде Басқару серверін жылдам іске қосу шеберінің жұмысы туралы ақпарат берілген.

Шеберге интернетке қатынасу керек. Басқару сервері интернетке қатынаса алмаса, шебердің барлық қадамдарын Kaspersky Security Center Web Console интерфейсі арқылы қолмен орындау ұсынылады.

Kaspersky Security Center бағдарламасы, желіні қауіпсіздік қауіптерінен қорғауды қамтамасыз ететін орталықтандырылған басқару жүйесін құру үшін қажетті параметрлердің ең аз жиынтығын конфигурациялауға мүмкіндік береді. Бұл конфигурация бағдарламаны жылдам іске қосу шеберінде орындалады. Шебердің жұмысы барысында, сіз бағдарламаға келесі өзгерістерді енгізе аласыз:

- Басқару топтарындағы құрылғыларға автоматты түрде таратуға болатын кілт файлдарын қосу немесе белсендіру кодтарын енгізу.
- Kaspersky Security Network (KSN) желісімен өзара әрекетті конфигурациялау. KSN қолдануға рұқсат берген кезде, шебер KSN және құрылғылар арасында өзара әрекетті қамтамасыз ететін KSN прокси-сервері қызметін қосады.
- Басқару сервері мен басқарылатын бағдарламалардың жұмысындағы оқиғалар туралы хабарландыруларды электрондық пошта арқылы таратуды конфигурациялаңыз (хабарландыру сәтті түрде келуі үшін Басқару серверінде және барлық алушы құрылғыларда Messenger хабар қызметі іске қосылуы керек).

- Жұмыс станциялары мен серверлерді қорғау саясатын, сондай-ақ зиянды БҚ іздеу, жаңартуларды алу және басқарылатын құрылғылар иерархиясының жоғарғы деңгейі үшін деректерді сақтық көшірмелеу тапсырмаларын қалыптастыру.

  Бағдарламаны жылдам іске қосу шебері **Басқарылатын құрылғылар** қалтасында саясаттары әлі жасалмаған бағдарламалар үшін ғана саясаттар жасайды. Осындай аттары бар тапсырмалар басқарылатын құрылғылар иерархиясының жоғары деңгейі үшін әлдеқашан жасалған болса, бағдарламаны жылдам іске қосу шебері мұндай тапсырмаларды жасамайды.

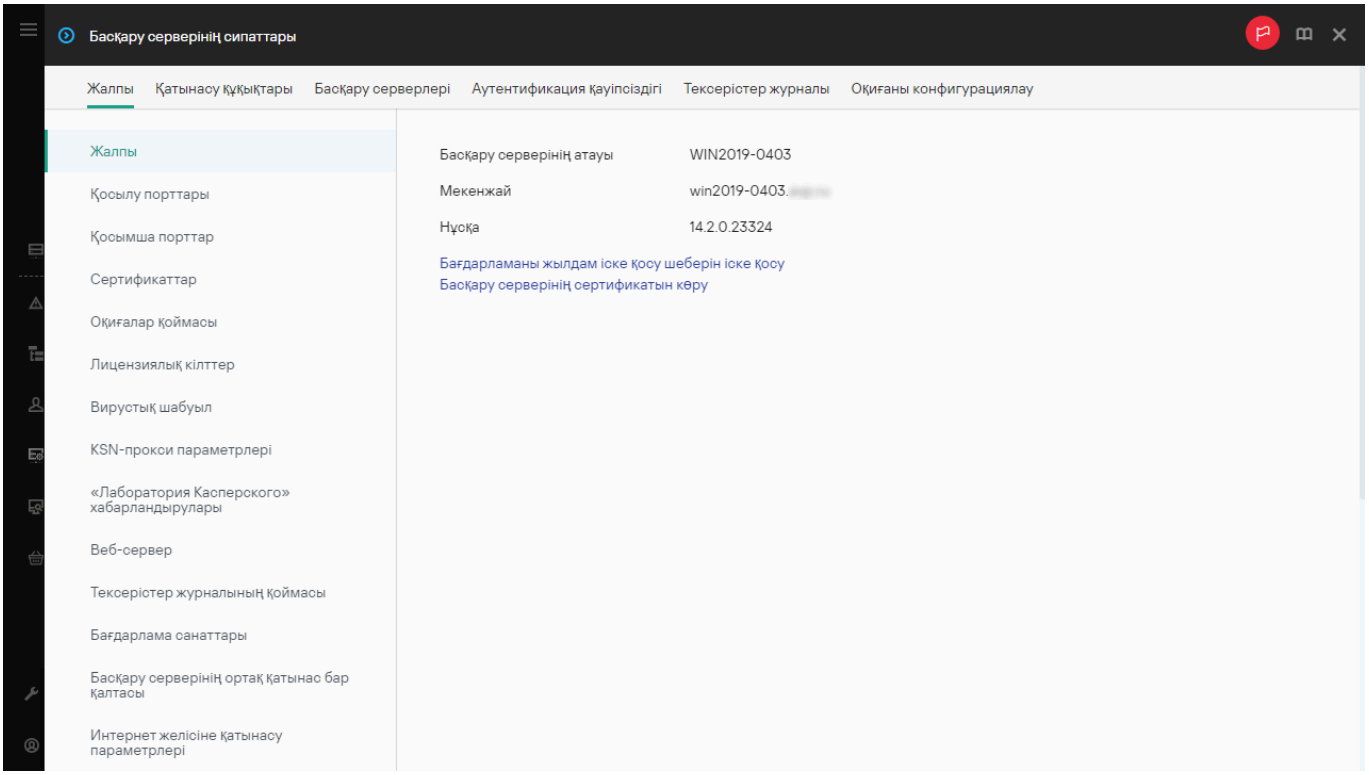
Серверге бірінші рет қосылу кезінде Басқару серверін орнатқаннан кейін, бағдарлама автоматты түрде бағдарламаны жылдам іске қосу шеберін іске қосуды ұсынады. Сондай-ақ, бағдарламаны жылдам іске қосу шеберін кез келген уақытта қолмен іске қоса аласыз.

Бағдарламаны жылдам іске қосу шеберін қолмен іске қосу үшін:

1. Басты мәзірде Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жалпы** бөлімін таңдаңыз.



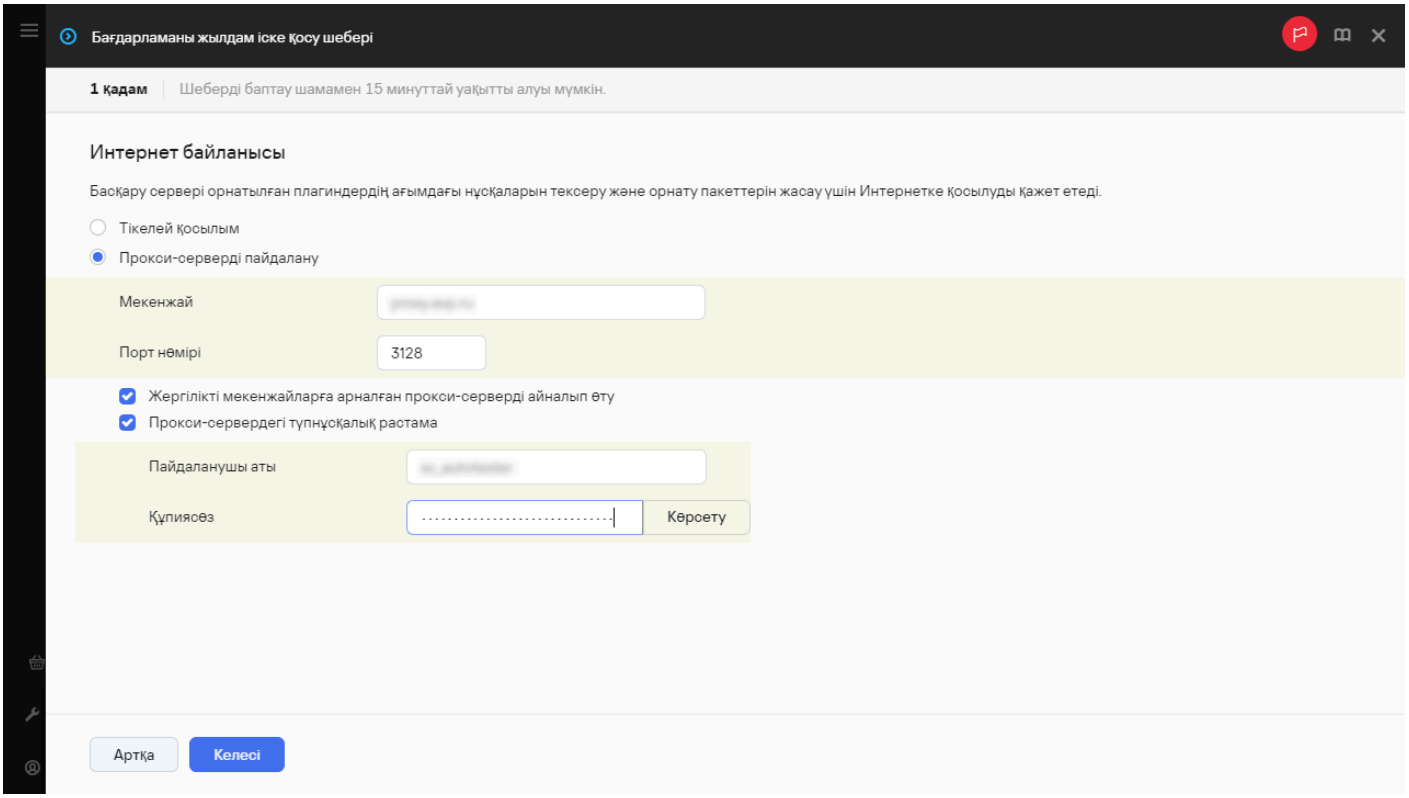
Басқару серверінің сипаттары терезесі

3. **Бағдарламаны жылдам іске қосу шеберін іске қосу** түймесін басыңыз.

Шебер Басқару серверін бастапқы конфигурациялауды ұсынады. Содан кейін, шебердің нұсқауларын орындаңыз. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

1-қадам. Интернетке қосылу параметрлерін көрсету

Басқару серверінің интернетке қатынасу параметрлерін көрсетіңіз. Kaspersky Security Network пайдалану, сондай-ақ Kaspersky Security Center және Kaspersky басқарылатын бағдарламалары үшін антивирустық дерекқорлар жаңартуларын жүктеу үшін интернетке қатынасуды конфигурациялау қажет.



Internet connection settings

Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін қосыңыз. Параметр қосулы болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

- **Мекенжай**

  Kaspersky Security Center-ді интернетке қосу үшін прокси-сервер мекенжайы.

- **Порт нөмірі**

  Kaspersky Security Center прокси-қосылымы орнатылатын порт нөмірі.

- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Жергілікті желідегі құрылғыларға қосылған кезде прокси-сервер қолданылмайды.

- **Прокси-сервердегі түпнұсқалық растама**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Прокси-серверді пайдалану жалаушасы қойылған болса, енгізу өрісі қолжетімді.

- **Пайдаланушы аты**

  Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

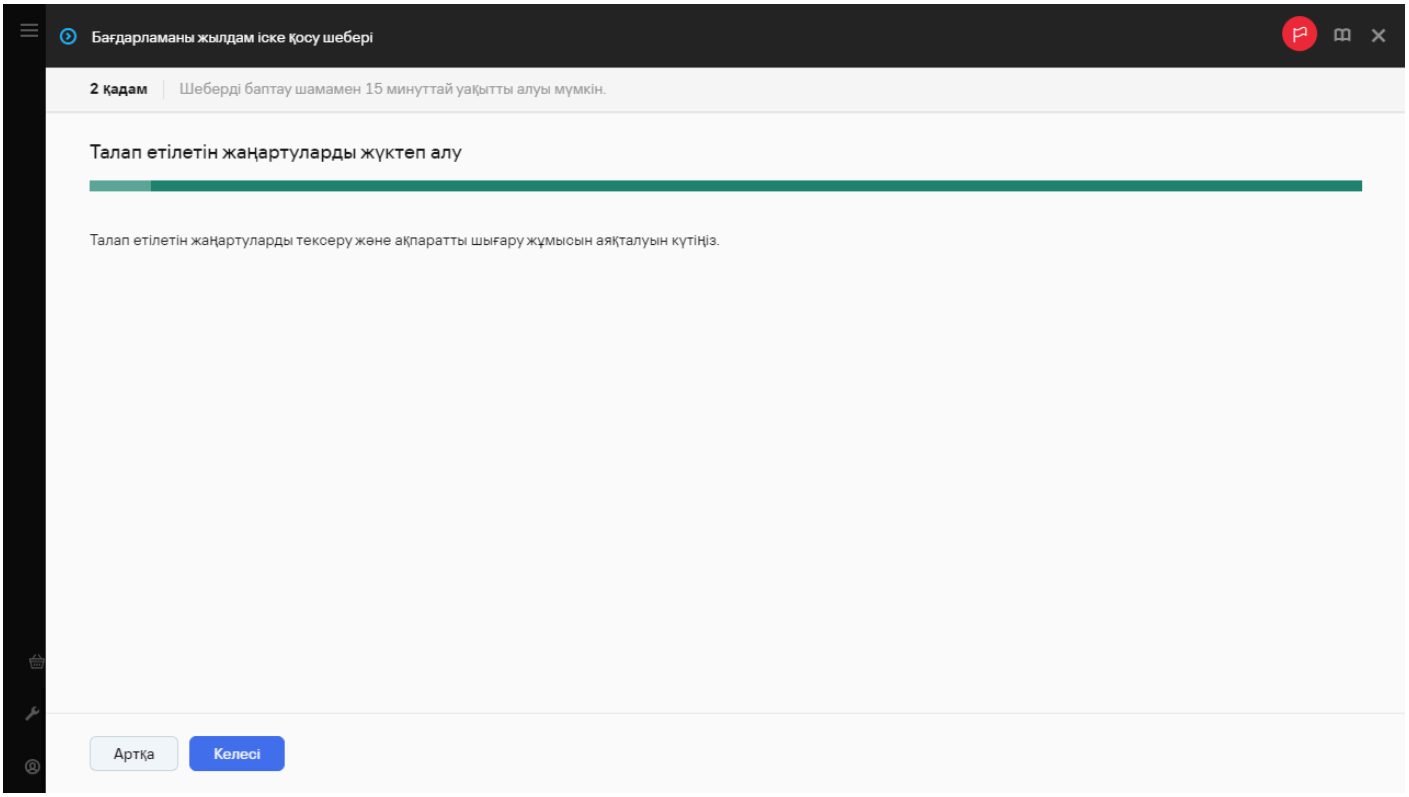
  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

Интернетке қатынасуды, бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, кейінірек конфигурациялай аласыз.

2-қадам. Талап етілетін жаңартуларды жүктеп алу

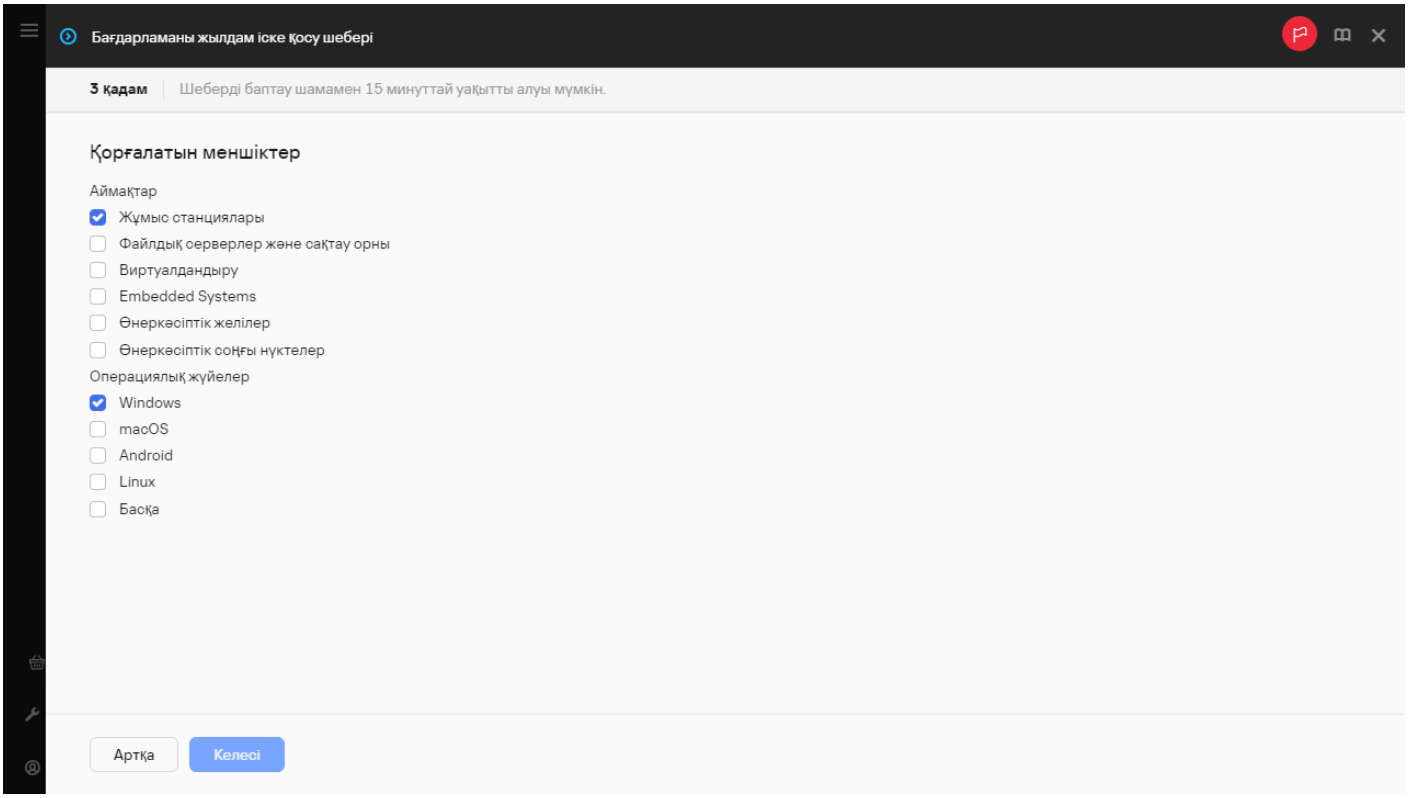
Қажетті жаңартулар Kaspersky серверлерінен автоматты түрде жүктеледі.



Талап етілетін жаңартуларды жүктеп алу

3-қадам. Қорғау үшін активтерді таңдау

Желіңізде қолданылатын қорғаныс аумақтары мен операциялық жүйелерді таңдаңыз. Осы параметрлерді таңдағанда, желіңіздегі клиент құрылғыларына орнату үшін жүктеуге болатын Kaspersky серверлеріндегі бағдарламаларды басқару плагиндері мен дистрибутивтеріне арналған сүзгілерді көрсетесіз.



Қорғау үшін активтерді таңдау

Келесі параметрлерді таңдаңыз:

- **Аймақтар**

  Сіз келесі қорғаныс аймақтарының бірін таңдай аласыз:

  - **Жұмыс станциялары**. Желідегі жұмыс станцияларын қорғағыңыз келсе, осы параметрді таңдаңыз. Әдепкі бойынша Жұмыс станциясы параметрі таңдалған.

  - **Файлдық серверлер және сақтау орны**. Желіңіздегі файл серверлерін қорғағыңыз келсе, осы параметрді таңдаңыз.

  - **Ұялы құрылғылар**. Ұйымыңызға немесе ұйымыңыздағы қызметкерлерге тиесілі мобильдік құрылғыларды қорғағыңыз келсе, осы параметрді таңдаңыз. Бұл параметрді таңдаған болсаңыз, бірақ Мобильдік құрылғыларды басқару мүмкіндігі бар лицензияны бермеген болсаңыз, мобильдік құрылғыларды басқару мүмкіндігі бар лицензияны беруді сұрайтын хабар көрсетіледі. Бұл лицензиясыз мобильдік құрылғыны басқару мүмкіндіктерін пайдалана алмайсыз.

  - **Виртуалдандыру**. Желіңіздегі виртуалды машиналарды қорғағыңыз келсе, осы параметрді таңдаңыз.

  - **Анти-спам**. Ұйымыңыздағы пошта серверлерін спамнан, алаяқтықтан және зиянды бағдарламаларды жеткізуден қорғағыңыз келсе, осы опцияны таңдаңыз.

- **Ендірілген жүйелер**. Банкоматтар (ATM) сияқты Windows операциялық жүйесімен жұмыс істейтін кіріктірілген жүйелерді қорғағыңыз келсе, осы параметрді таңдаңыз.

- **Өнеркәсіптік желілер**. Қауіпсіздік деректерін өнеркәсіптік желідегі және Kaspersky бағдарламаларымен қорғалған желілік соңғы құрылғылардан бақылағыңыз келсе, осы параметрді таңдаңыз.

- **Өнеркәсіптік соңғы нүктелер**. Өнеркәсіптік желінің бөлек түйіндерін қорғағыңыз келсе, осы параметрді таңдаңыз.

- **Операциялық жүйелер**

  Сіз келесі платформалардың бірін таңдай аласыз:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Басқа

  Операциялық жүйелердің қолдау көрсетілетін нұсқалары туралы қосымша ақпаратты Kaspersky Security Center Web Console аппараттық және бағдарламалық талаптары бөлімінен қараңыз.

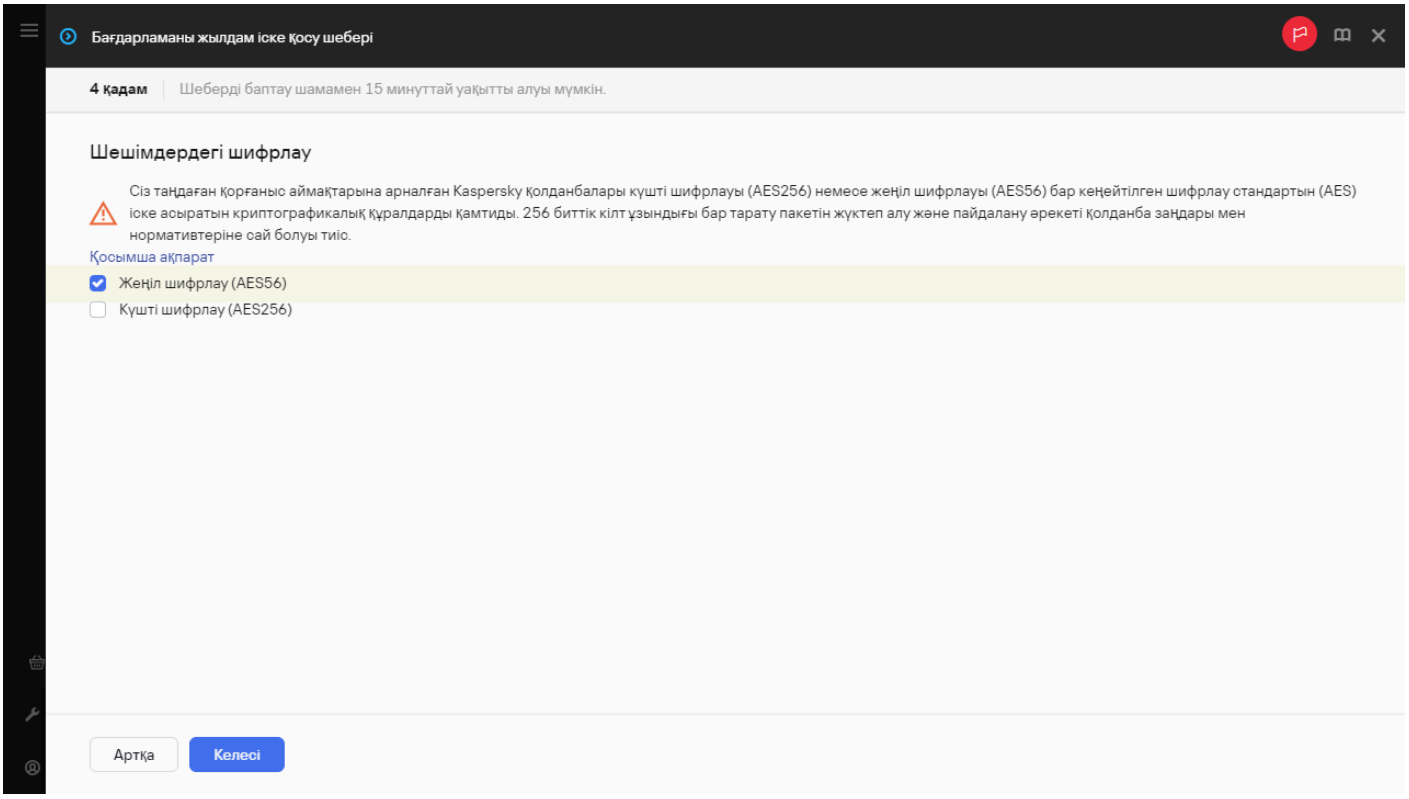
Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қолжетімді орнату пакеттерінің тізімінен Kaspersky бағдарламаларының орнату пакеттерін таңдауға болады. Қажетті орнату пакеттерін табуды жеңілдету үшін қолжетімді орнату пакеттерінің тізімін әртүрлі критерийлер бойынша сүзуге болады.

4-қадам. Шифрлауды таңдау

Шешімдердегі шифрлау терезесі, қорғаныс аумағы ретінде **Жұмыс станциялары** нұсқасы таңдалса ғана көрсетіледі.

Kaspersky Endpoint Security for Windows бағдарламасы, Windows операциялық жүйесі орнатылған клиент құрылғыларында сақталатын ақпаратты шифрлау аспаптарын қамтиды. Бұл шифрлау құралдарында, 256 биттік немесе 56 биттік кілттің ұзындығымен іске асырылған кеңейтілген шифрлау стандарты (AES) бар.

256 биттік кілт ұзындығы бар дистрибутивті жүктеу және пайдалану қолданыстағы заңдар мен ережелерге сәйкес жүзеге асырылуы керек. Ұйымыңыздың қажеттіліктері үшін жарамды Kaspersky Endpoint Security for Windows дистрибутивін жүктеп алу үшін ұйымыңыздың клиент құрылғылары орналасқан елдің заңнамасын қараңыз.



Шифрлауды таңдау

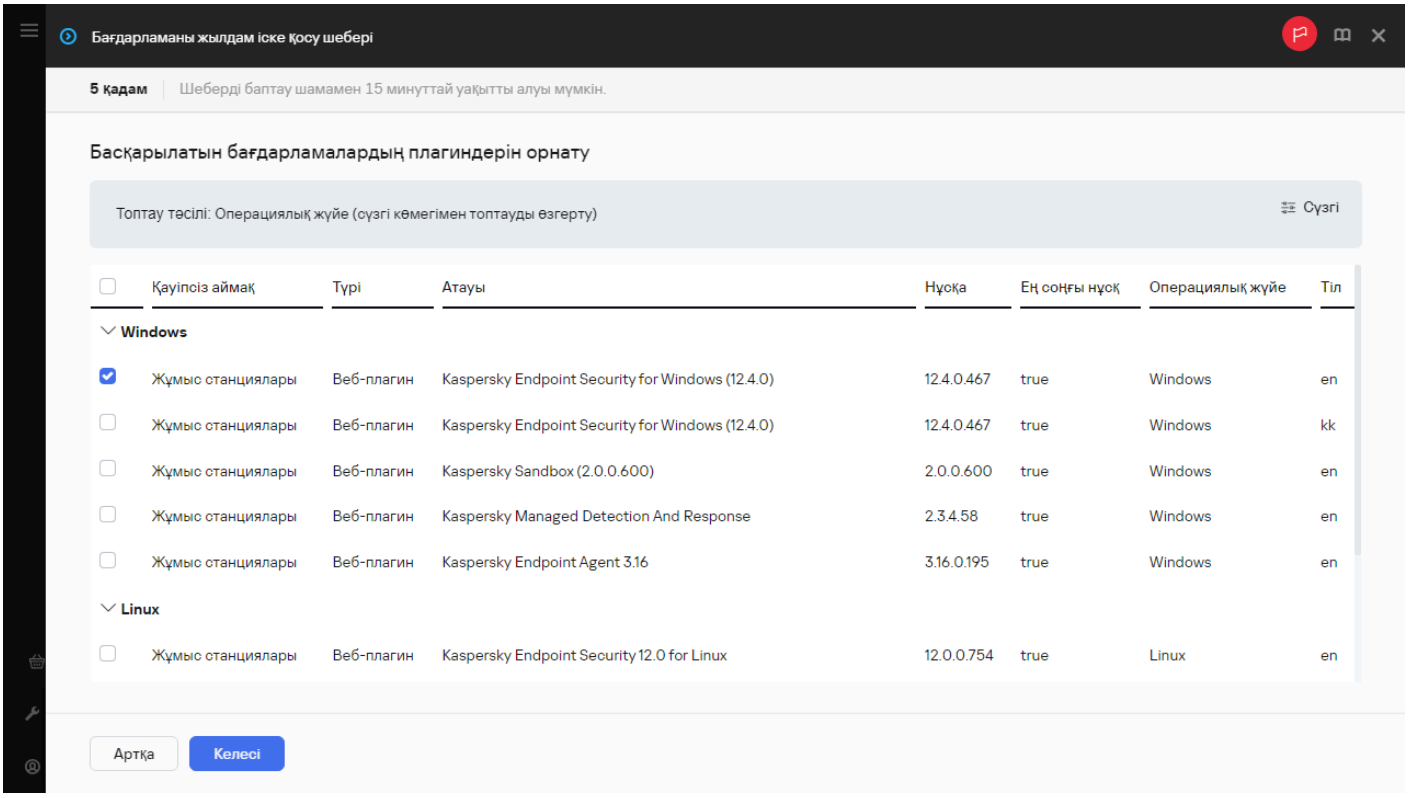
Шешімдердегі шифрлау терезесінде келесі шифрлау түрлерінің бірін таңдаңыз:

- Жылдам шифрлау. Осы шифрлау түрі үшін 56 разрядты кілт қолданылады.
- Тұрақты шифрлау. Осы шифрлау түрі үшін 256 разрядты кілт қолданылады.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қажетті шифрлау түрі бар Kaspersky Endpoint Security for Windows дистрибутивін кейінірек таңдауға болады.

5-қадам. Басқарылатын бағдарламалардың плагиндерін орнатуды конфигурациялау

Орнату үшін басқарылатын бағдарламалардың плагиндерін таңдаңыз. Kaspersky серверлерінде орналасқан плагиндер тізімі көрсетіледі. Тізім шебердің алдыңғы қадамында таңдалған параметрлерге сәйкес сүзгіленген. Әдепкі бойынша, барлық тілдердің плагиндері толық тізімге енгізілген. Таңдалған тілде тек плагинді көрсету үшін сүзгіні пайдаланыңыз.



Басқарылатын қолданбалардың плагиндерін орнату

Плагиндер тізімі келесі бағандарды қамтиды:

- **Қауіпсіз аймақ**

  Бұл бағаң қорғау үшін таңдалған аумақтарды көрсетеді.

- **Түрі**

  Бұл бағаң плагин түрлерін көрсетеді.

- **Атауы**

  Қосылатын модульдер, алдыңғы қадамда таңдалған қорғаныс аумақтары мен платформаларына байланысты таңдалды.

- **Нұсқа**

  Тізімге Kaspersky серверлерінде орналастырылған плагиндердің барлық нұсқалары қосылған. Әдепкі бойынша плагиндердің соңғы нұсқалары таңдалған.

- **Ең соңғы нұсқ**

  Бұл баған плагиннің соңғы нұсқасы екенін көрсетеді. Егер **true** мәні көрсетілсе, тиісті плагиннің соңғы нұсқасы бар. Егер **false** мәні көрсетілсе, тиісті плагиннің кейінгі нұсқасы бар.

- **Операциялық жүйе**

  Бұл баған операциялық жүйелердің плагиндерін көрсетеді.

- **Тіл**

  Әдепкі бойынша, плагинді локализациялау тілі, орнату кезінде таңдалған Kaspersky Security Center тіліне байланысты. Басқа тілдерді **Басқару консолінің тілін көрсету немесе** ашылмалы тізімінен таңдауға болады.

Қосылатын модульдерді таңдау үшін, орнатуды бастау мақсатымен **Келесі** түймесін басыңыз.

Kaspersky бағдарламалары үшін басқару плагиндерін бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, кейінірек қолмен орнатуға болады.

Бағдарламаны жылдам іске қосу шебері таңдалған плагиндерді автоматты түрде орнатады. Кейбір плагиндерді орнату үшін сіз Лицензиялық келісімнің шарттарын қабылдауыңыз қажет. Экранда көрсетілетін Лицензиялық келісімнің мәтінімен танысып шығыңыз, **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** жалаушасын қойыңыз және **Орнату** түймесін басыңыз. Лицензиялық келісімнің шарттарымен келіспесеңіз, плагин орнатылмайды.

Барлық таңдалған плагиндер орнатылғаннан кейін, бағдарламаны жылдам іске қосу шебері автоматты түрде келесі қадамға өтеді.

6-қадам. Таңдалған плагиндерді орнату

Бастапқы орнату шебері алдыңғы қадамда таңдалған плагиндерді автоматты түрде орнатады. Кейбір плагиндерді орнату үшін сіз Лицензиялық келісімнің шарттарын қабылдауыңыз қажет. Экранда көрсетілетін Лицензиялық келісімнің мәтінімен танысып шығыңыз, **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** жалаушасын қойыңыз және **Орнату** түймесін басыңыз. Лицензиялық келісімнің шарттарымен келіспесеңіз, плагин орнатылмайды.

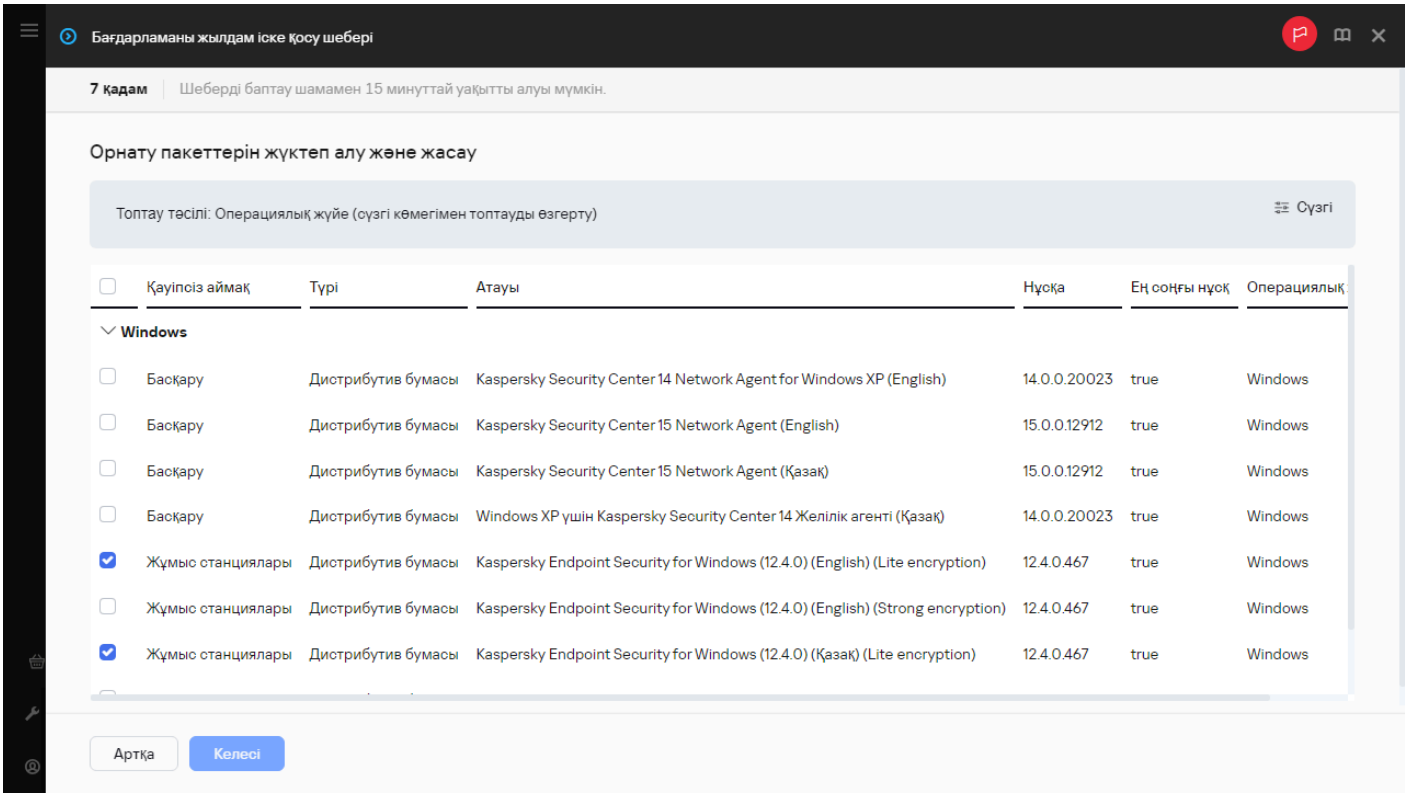
Барлық таңдалған плагиндер орнатылғаннан кейін, бағдарламаны жылдам іске қосу шебері автоматты түрде келесі қадамға өтеді.

7-қадам. Дистрибутивтерді жүктеу және орнату пакеттерін жасау

Жүктелетін дистрибутивті таңдаңыз.

Басқарылатын бағдарламалардың дистрибутивтері үшін Kaspersky Security Center белгілі бір минималды нұсқасын орнату қажет болуы мүмкін.

Kaspersky Endpoint Security for Windows үшін шифрлау түрі таңдалғаннан кейін, екі шифрлау түрі үшін дистрибутивтер тізімі көрсетіледі. Тізімнен таңдалған шифрлау түрі бар дистрибутив таңдалады. Сіз кез келген шифрлау түрі үшін дистрибутивті таңдай аласыз. Дистрибутив тілі Kaspersky Security Center тіліне сәйкес келеді. Kaspersky Security Center тілі үшін Kaspersky Endpoint Security for Windows дистрибутиві болмаса, ағылшын тіліндегі дистрибутив таңдалады.



Дистрибутивтерді жүктеу және орнату пакеттерін жасау

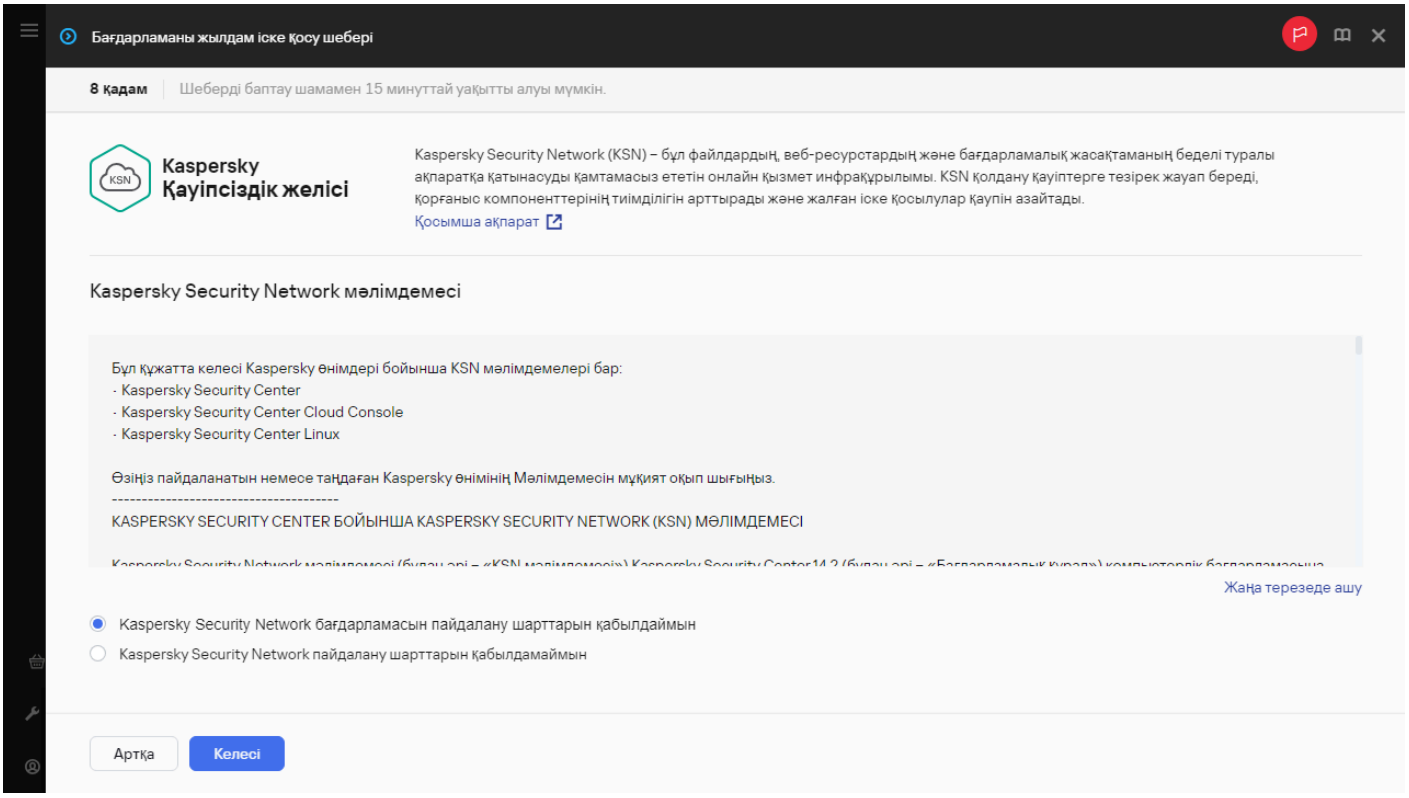
Кейбір дистрибутивтерді жүктеуді аяқтау үшін сіз Лицензиялық келісімді қабылдауыңыз керек. **Қабылдау** түймесін басқан кезде Лицензиялық келісім мәтіні көрсетіледі. Шебердің келесі қадамына өту үшін сіз Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ Kaspersky Құпиялылық саясатының шарттарын қабылдауыңыз керек. Егер сіз ережелер мен шарттарды қабылдамасаңыз, пакетті жүктелмейді.

Лицензиялық келісімнің ережелері мен шарттарын, сондай-ақ Kaspersky Құпиялылық саясатының шарттарын қабылдағаннан кейін, дистрибутивтерді жүктеу жалғасады. Болашақта орнату пакеттерін клиент құрылғыларында Kaspersky бағдарламаларын орналастыру үшін пайдалануға болады.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, дистрибутивтерді жүктеп алуды және орнату пакеттерін жасауды кейінірек орындауға болады.

8-қадам. Kaspersky Security Network конфигурациялау

Kaspersky Security Center жұмысы туралы ақпаратты Kaspersky Security Network білім базасына беру параметрлерін конфигурациялаңыз.



Kaspersky Security Network конфигурациялау

Келесі нұсқалардың бірін таңдаңыз:

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын**

  Kaspersky Security Center және клиент құрылғыларында орнатылған басқарылатын бағдарламалар, олардың жұмысы туралы ақпаратты Kaspersky Security Network қызметіне автоматты режимде жіберетін болады. Kaspersky Security Network-пен ынтымақтастық, вирустар мен қауіптер туралы дерекқорды барынша жылдам жаңартуды қамтамасыз ете отырып, туындаған қауіпсіздік қауіптеріне жауап беру жылдамдығын арттырады.

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдамаймын**

  Kaspersky Security Center және басқарылатын бағдарламалар өз жұмысы туралы ақпаратты Kaspersky Security Network қызметіне жібермейді.

  Осы параметрді таңдасаңыз, Kaspersky Security Network қызметі өшіріледі.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ Kaspersky Security Network (KSN) жүйесіне қатынасуды кейінірек конфигурациялауға болады.

9-қадам. Бағдарламаны белсендіру тәсілін таңдау

Kaspersky Security Center белсендірудің келесі нұсқаларының бірін таңдаңыз:

- **Белсендіру кодыңызды енгізіңіз**

  Белсендіру коды – жиырма латын әрпі мен санынан құралған бірегей бірізділік. Сіз Kaspersky Security Center бағдарламасын белсендіретін кілтті қосу үшін белсендіру кодын енгізесіз. Белсендіру коды сізге Kaspersky Security Center сатып алу кезінде көрсетілген электрондық пошта мекенжайына жіберіледі.

  Бағдарламаны белсендіру кодының көмегімен белсендіру үшін, Kaspersky белсендіру серверлеріне қосылу мақсатында интернетке қатынасу талап етіледі.

  Бағдарламаны белсендіру үшін осы нұсқаны таңдасаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосуға болады.

  Осы нұсқа таңдалса, лицензиялық кілт басқарылатын құрылғыларға таратылатын болады.

  Осы нұсқа таңдалмаса, лицензиялық кілтті басқарылатын құрылғыларға, басқару консолі шежіресінің **Kaspersky лицензиялары** қалтасында кейінірек таратуға болады.

- **Кілт файлын көрсетіңіз**

  Кілт файлы – Kaspersky сізге ұсынатын key кеңейтімі бар файл. Кілт файлы бағдарламаны белсендіретін кілтті қосуға арналған.

  Кілт файлын алу әдістері Кілт файлы туралы ақпарат бөлімде сипатталған.

  Бағдарламаны кілт файлы арқылы белсендіру үшін Kaspersky белсендіру серверлеріне қосылудың қажет емес.

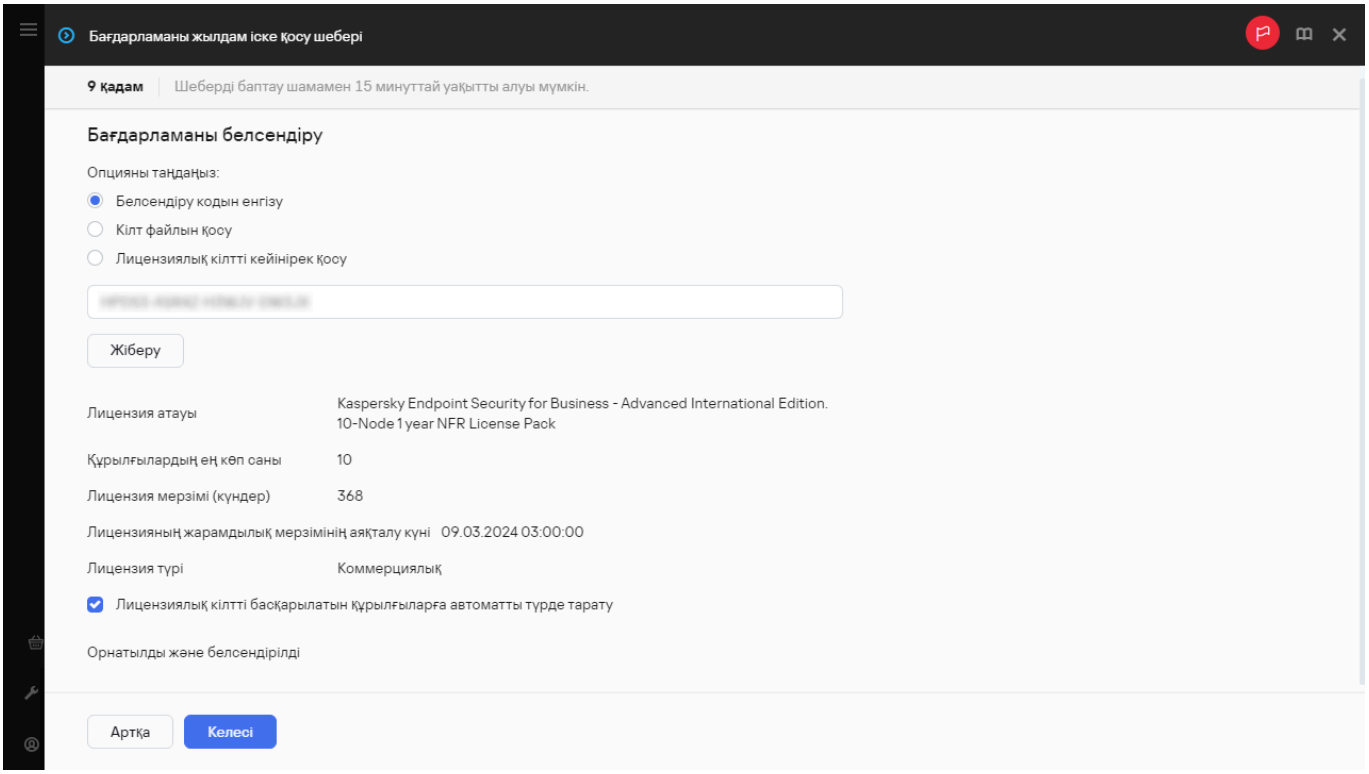
  Бағдарламаны белсендіру үшін осы нұсқаны таңдасаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосуға болады.

  Осы нұсқа таңдалса, лицензиялық кілт басқарылатын құрылғыларға таратылатын болады.

  Осы нұсқа таңдалмаса, лицензиялық кілтті басқарылатын құрылғыларға, басқару консолі шежіресінің **Kaspersky лицензиялары** қалтасында кейінірек таратуға болады.

- **Бағдарламаны белсендіруді кейінге қалдырыңыз**

  Бағдарлама Базалық функционалдылық режимінде, Ұялы құрылғыларды басқару және Осалдықтар мен патчтарды басқару қызметінің қолдауынсыз жұмыс істейтін болады.



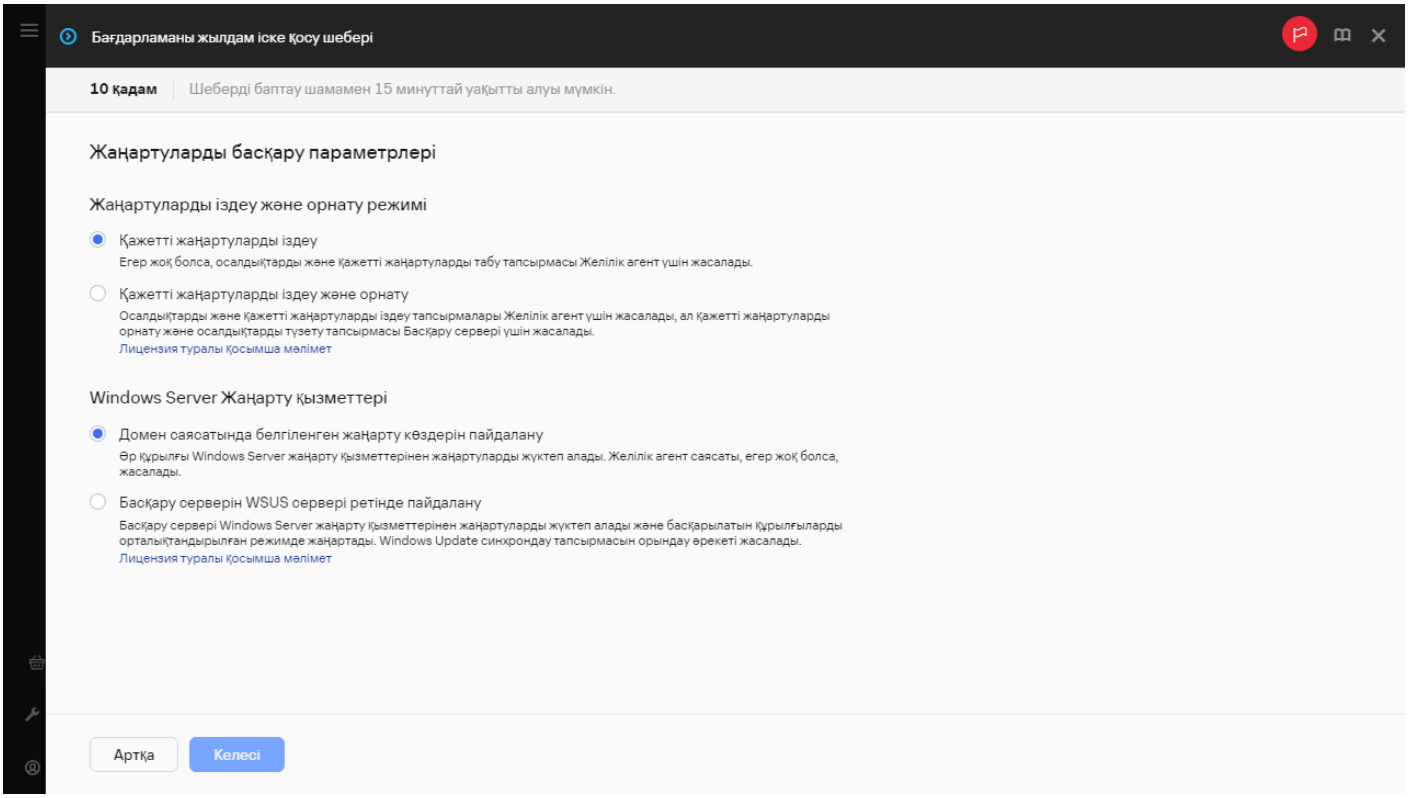
Бағдарламаны белсендіру тәсілін таңдау

Бағдарламаны белсендіруді кейінге қалдырсаңыз, **Операциялар** → **Лицензиялау** тармағын таңдап, кілтті кейін кез келген уақытта қоса аласыз.

AMI дайын кескінінен немесе SKU қолдану үшін ай сайынғы шоттарды қолдану арқылы орналастырылған Kaspersky Security Center бағдарламасымен жұмыс істеу кезінде, сіз кілт файлын көрсете алмайсыз немесе белсендіру кодын енгізе алмайсыз.

10-қадам. Үшінші тарап бағдарламаларының жаңартуларын басқару параметрлерін көрсету

Осалдықтар мен патчтарды басқаруға арналған лицензия болмаса және *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы бұрыннан бар болса, бұл қадам көрсетілмейді.



Үшінші тарап жаңартуларын басқару параметрлері

Үшінші тарап бағдарламаларын жаңарту үшін келесі нұсқалардың бірін таңдаңыз:

- **Қажетті жаңартуларды іздеу**

  Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бұрын жасалмаған болса, автоматты түрде жасалады.

  Әдепкі бойынша, осы нұсқа таңдалады.

- **Қажетті жаңартуларды іздеу және орнату**

  Осалдықтарды және қажетті жаңартуларды іздеу және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмалары бұған дейін жасалмаған болса, автоматты түрде жасалады.

  Бұл параметр Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда қолжетімді.

Windows Update жаңартулары үшін келесі нұсқалардың бірін таңдаңыз:

- **Домен саясатында белгіленген жаңарту көздерін пайдалану**

  Windows Update жаңартулары клиент құрылғыларына домен саясаты параметрлеріне сай жүктеледі. Желілік агент саясаты бұрын жасалмаған болса, автоматты түрде жасалады.

- **Басқару серверін WSUS сервері ретінде пайдалану**

  Windows Update жаңартулары клиент құрылғыларына Басқару серверінен жүктеледі. *Windows Update жаңартуларын синхрондау* тапсырмасы және Желілік агент саясаты бұған дейін жасалмаған болса, автоматты түрде жасалады.

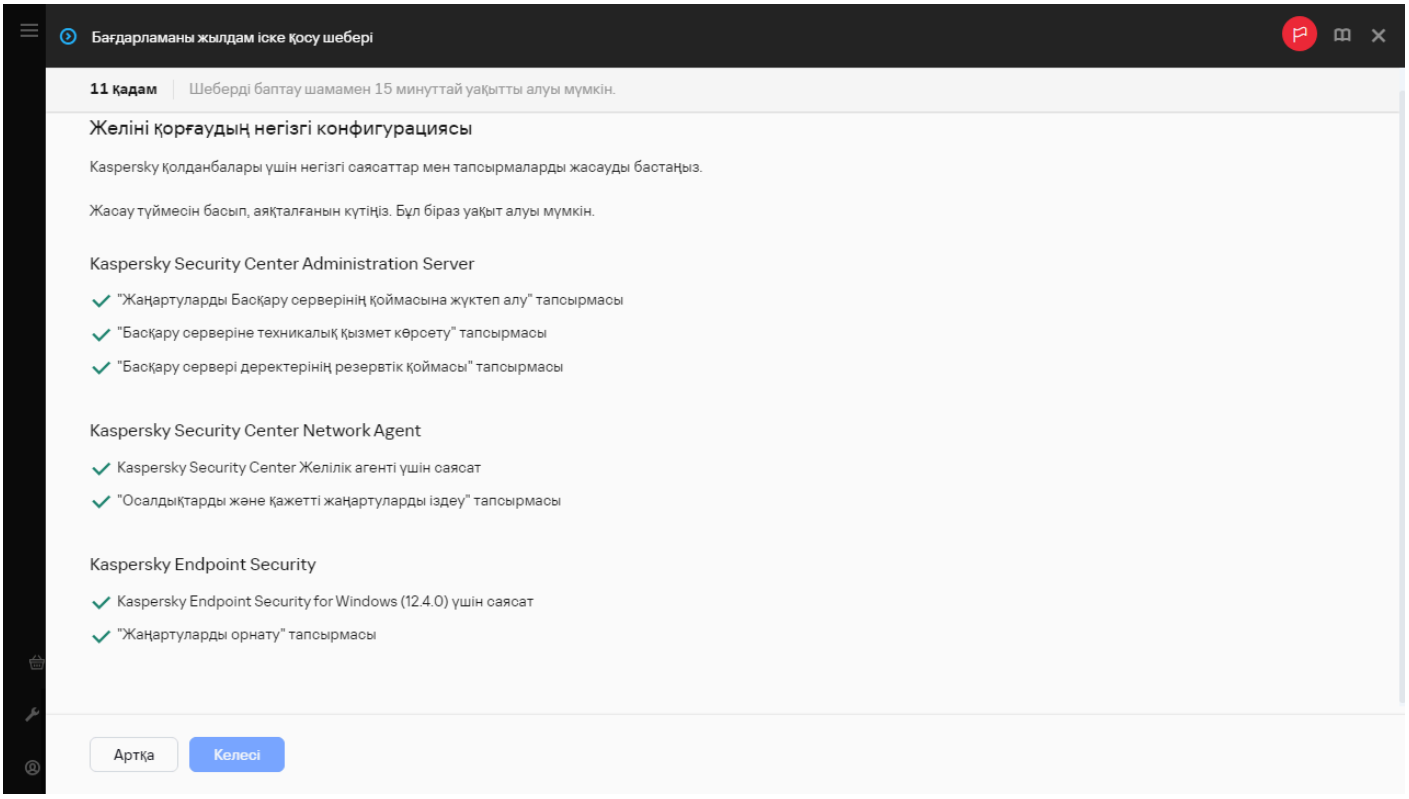
  Бұл параметр Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда қолжетімді.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ *Осалдықтарды және қажетті жаңартуларды іздеуді жасауға* және *Қажетті жаңартуларды орнатуға және осалдықтарды түзетуге* болады. Басқару серверін WSUS сервері ретінде қолдану үшін сізге *Windows Update жаңартуларын синхрондау* тапсырмасын жасап, Желілік агент саясатында **Басқару серверін WSUS сервері ретінде пайдалану** параметрін таңдау керек.

11-қадам. Желі қорғанысының базалық конфигурациясын жасау

Сіз жасалған саясаттар мен тапсырмалардың тізімін тексере аласыз.

Шебердің келесі қадамына өту үшін саясаттар мен тапсырмалардың жасалуының аяқталуын күтіңіз.

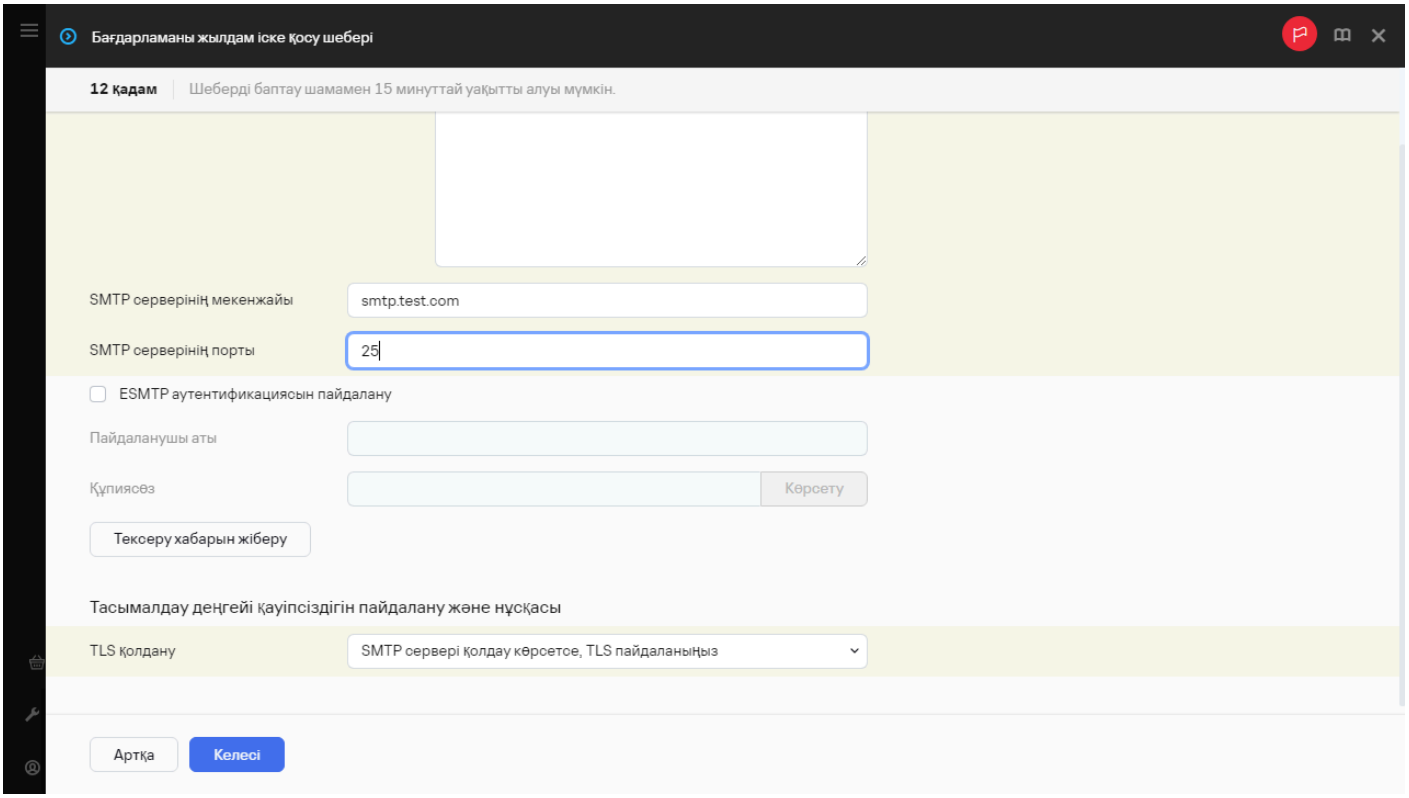


Желі қорғанысының базалық конфигурациясын жасау

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, қажетті тапсырмалар мен саясаттарды кейінірек жасауға болады.

12-қадам. Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Клиент құрылғыларында Kaspersky бағдарламалары жұмыс істеген кезде тіркелетін оқиғалар туралы хабарландыру тарату параметрлерін конфигурациялаңыз. Бұл параметрлер бағдарламалардың саясаттарында әдепкі бойынша мәндер ретінде пайдаланылады.



Электрондық пошта арқылы хабарландыруларды жіберу әдісін конфигурациялау

Kaspersky бағдарламаларының туындайтын оқиғалары туралы хабарландырулар таратылымын конфигурациялау үшін келесі параметрлер қолжетімді:

- **Алушылар (электрондық пошта мекенжайлары)**

  Бағдарлама хабарландыру жіберетін пайдаланушылардың электрондық пошта мекенжайлары. Бір не бірнеше мекенжайды енгізуге болады; бірнеше мекенжай енгізілсе, оларды нүктелі үтірмен бөліңіз.

- **SMTP серверінің мекенжайы**

  Ұйымыңыздың пошта серверлерінің мекенжайы немесе мекенжайлары.

  Бірнеше мекенжайды көрсетсеңіз, оларды үтірлі нүктемен бөліңіз. Келесі параметр мәндерін пайдалануыңызға болады:

  - IPv4 мекенжайы немесе IPv6 мекенжайы;
  - Windows желісіндегі құрылғының атауы (NetBIOS атауы);
  - SMTP сервері DNS атауы.

- **SMTP серверінің порты**

  SMTP серверінің коммуникациялық портының нөмірі. Бірнеше SMTP серверін қолдансаңыз, олармен қосылым көрсетілген коммуникациялық порт арқылы орнатылады. Әдепкі бойынша 25-порт орнатылған.

- **ESMTP аутентификациясын пайдалану**

  ESMTP аутентификациясын қолдауды қосу. Жалаушаны қойғаннан кейін, ESMTP аутентификациясы параметрлерін **Пайдаланушы аты** және **Құпиясөз** өрістерінде көрсетуге болады. Әдепкі бойынша, жалауша алынып тасталған.

- **TLS қолдану**

  SMTP сервері үшін TLS қосылым параметрлерін көрсетуіңізге болады:

  - **TLS пайдаланбау**

    Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

  - **SMTP сервері қолдау көрсетсе, TLS пайдаланыңыз**

    SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

  - **Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз**

    TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

    > Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

    Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз мәнін таңдасаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

  Сіз **Сертификаттарды көрсету** сілтемесінен өтіп, TLS қосылымы үшін сертификатты көрсете аласыз:

  - SMTP серверінің сертификаты файлын таңдаңыз:

    Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

  - Клиент сертификаты файлын таңдаңыз:

    Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

    - X.509 сертификаты:

      Сертификаты бар файлды және жеке кілт файлын көрсетуіңіз қажет. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- pkcs12 контейнері:

  Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

Электрондық пошта хабарлары туралы хабарландыру параметрлерін **Тексеру хабарын жіберу** түймесі арқылы тексеруге болады.

Оқиға хабарландыруларын, бағдарламаны жылдам іске қосу шеберін іске қоспай-аяқ, кейінірек конфигурациялай аласыз.

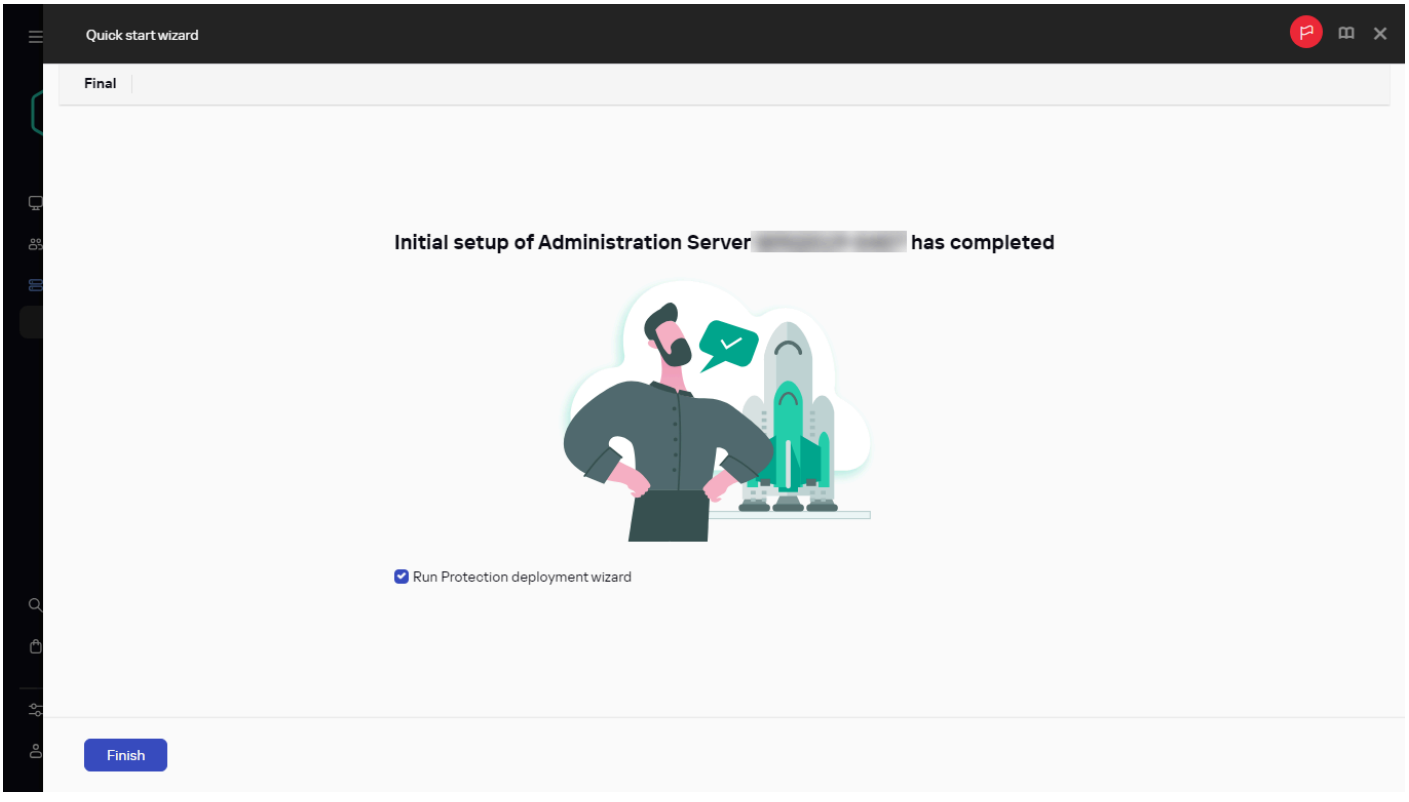
13-қадам. Желіде сауалнама өткізу

Басқару сервері бастапқы желі сауалнамасын орындайды. Сауалнама барысында оны орындау барысы көрсетіледі. Сауалнама аяқталғаннан кейін, **Анықталған құрылғыларды қарап шығу** сілтемесі қолжетімді болады. Басқару сервері анықтаған желі құрылғыларын қарап шығу үшін сілтеме арқылы өтуіңізге болады. Жылдам іске қосу шеберіне оралу үшін **Escape** пернесін басыңыз.

Бағдарламаны жылдам іске қосу шеберін іске қоспай-ақ, желіде кейінірек сауалнама өткізуге болады. Kaspersky Security Center Web Console көмегімен домен контроллерлері, Windows домендері, IP ауқымдары және IPv6 желілері сауалнамасын реттеңіз.

14-қадам. Бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау

Антивирустық бағдарламаларды немесе Желілік агентті желіңіздегі құрылғыларға автоматты түрде орнатуды іске қосқыңыз келсе, бағдарламаны жылдам іске қосу шеберінің жұмысын аяқтау бетінде **Қорғанысты орналастыру шеберін іске қосу** жалаушасын қойыңыз.



Бастапқы орнату шеберінің соңғы қадамы

Шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Автономды құрылғыларды қосу

Бұл бөлімде автономды құрылғыларды Басқару серверіне қалай қосу керектігі сипатталған (яғни, негізгі желіден тыс басқарылатын құрылғылар).

Сценарий: Автономды құрылғыларды қосылым шлюзі арқылы қосу

Бұл сценарийде, негізгі желіден тыс басқарылатын құрылғыларды Басқару серверіне қалай қосу керектігі сипатталған.

Алдын ала талаптар

Сценарийде келесі алдын ала талаптар бар:

- Сіздің ұйымыңыздың желісінде демилитаризацияланған аймақ (DMZ) ұйымдастырылған.
- Kaspersky Security Center Басқару сервері корпоративтік желіде орналастырылған.

Кезеңдер

Бұл сценарий келесі кезеңдерден тұрады:

1. **Демилитаризацияланған аймақта клиент құрылғысын таңдау**

   Бұл құрылғы қосылым шлюзі ретінде пайдаланылады. Таңдалған құрылғы қосылым шлюздерінің талаптарына сай болуы керек.

2. **Желілік агентті қосылым шлюзі ретінде орнату**

   Таңдалған құрылғыға Желілік агентті орнату үшін жергілікті орнатуды пайдалануды ұсынамыз.

   Әдепкі бойынша орнату файлы келесі мекенжай бойынша орналасқан: \\<Сервер атауы>\KLSHARE\PkgInst\NetAgent_<нұсқа нөмірі>.

   Желілік агентті орнату шеберінің **Қосылым шлюзі** терезесінде **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** параметрін таңдаңыз. Бұл режим бір уақытта қосылым шлюзінің рөлін белсендіреді және Желілік агентке Басқару серверіне қосылуды емес, Басқару серверінен қосылуды күтуді бұйырады.

   Болмаса желілік агентті Linux құрылғысына орнатып, желілік агентті қосылым шлюзі ретінде жұмыс істейтіндей конфигурациялауға болады, бірақ Linux құрылғыларында жұмыс істейтін желілік агент шектеулерінің тізіміне назар аударыңыз.

3 Қосылым шлюзінің желілік экранында қосылымдарға рұқсат беру

Басқару сервері демилитаризацияланған аймақтағы қосылым шлюзіне қосыла алуы үшін, Басқару сервері мен қосылым шлюзі арасындағы барлық желілік экрандарда 13000 TCP портына қосылуға рұқсат етіңіз.

Егер қосылым шлюзі интернетте нақты IP мекенжайына ие болмаса, бірақ мұның орнына Network Address Translation (бұдан әрі NAT) артында орналасса, NAT арқылы қосылымдарды жіберу ережесін конфигурациялаңыз.

4 Сыртқы құрылғылар үшін басқару тобын құру

Басқарылатын құрылғылар тобы ішінде топ жасаңыз. Бұл жаңа топта сыртқы басқарылатын құрылғылар болады.

5 Қосылым шлюзін Басқару серверіне қосу

Сіз конфигурациялаған қосылым шлюзі Басқару серверінен қосылымды күтеді. Алайда, Басқару сервері басқарылатын құрылғылар арасында қосылым шлюзі бар құрылғыны атап көрсетпейді. Мұның себебі, қосылым шлюзі Басқару серверімен байланыс орнатуға тырыспады. Сол себепті, Басқару сервері қосылым шлюзіне қосылуды бастау үшін сізге арнайы процедура қажет болады.

Келесі әрекеттерді орындаңыз:

1. Қосылым шлюзін тарату нүктесі ретінде қосыңыз.
2. Қосылым шлюзін **Тағайындалмаған құрылғылар** тобынан сыртқы құрылғылар үшін құрылға топқа жылжытыңыз.

Қосылым шлюзі қосылған және конфигурацияланған.

6 Сыртқы компьютер құрылғыларын басқару серверіне қосу

Әдетте сыртқы компьютер құрылғылары желінің периметрі ішінде жылжытылмайды. Сондықтан, Желілік агентті орнату кезінде оларды қосылым шлюзі арқылы Басқару серверіне қосу үшін конфигурациялау керек.

7 Сыртқы компьютер құрылғыларының жаңартуларын реттеу

Қауіпсіздік қолданбаларының жаңартулары басқару серверінен жүктеп алынатындай конфигурацияланған болса, сыртқы құрылғылар жаңартуларды қосылым шлюзі арқылы жүктеп алады. Мұның екі кемшілігі бар:

- Бұл компанияның интернет-арнасының өткізу қабілеттілігін алатын артық трафик.
- Бұл жаңартуларды алудың ең жылдам тәсілі емес. Сыртқы құрылғылар үшін Kaspersky жаңарту серверлерінен жаңартуларды алу арзан әрі жылдам болуы мүмкін.

Келесі әрекеттерді орындаңыз:

1. Барлық сыртқы құрылғыны бұрын жасалған жеке басқару тобына жылжытыңыз.
2. Жаңарту тапсырмасынан сыртқы құрылғылары бар топты алып тастау.
3. Сыртқы құрылғылары бар топ үшін бөлек жаңарту тапсырмасын жасаңыз.

8 Ноутбуктерді Басқару серверіне қосу

Кейде ноутбуктер желіде, ал басқа уақытта – желіден тыс болады. Тиімді басқару үшін, олардың орналасқан жеріне байланысты Басқару серверіне басқаша қосылуы қажет. Трафикті тиімді пайдалану үшін олар орналасқан жеріне байланысты әртүрлі көздерден жаңартуларды алуы керек.

Сізге автономды пайдаланушыларға арналған ережелерді конфигурациялау керек: қосылым профильдері және желілік орналасу сипаттамалары. Әрбір ереже ноутбуктер орналасқан жеріне қарай қосылатын Басқару серверінің үлгісін және олар жаңартуларды алуы тиісті Басқару серверінің үлгісін анықтайды.

Сценарий: демилитаризацияланған аймақтағы Басқару сервері арқылы автономды құрылғыларды қосу

Негізгі желіден тыс орналасқан басқарылатын құрылғыларды Басқару серверіне қосқыңыз келсе, оны демилитаризияланған аймақта (DMZ) орналасқан басқарылатын Басқару сервері арқылы орындауға болады.

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Сіздің ұйымыңыздың желісінде демилитаризацияланған аймақ (DMZ) ұйымдастырылған.
- Kaspersky Security Center Басқару сервері ұйымның ішкі желісінде орналастырылған.

Кезеңдер

Бұл сценарий келесі кезеңдерден тұрады:

1. **Демилитаризацияланған аймақта клиент құрылғысын таңдау**

   Демилитаризацияланған аймақта (DMZ) қосалқы Басқару сервері ретінде пайдаланылатын клиент құрылғысын таңдаңыз.

2. **Kaspersky Security Center Басқару серверін орнату.**

   Осы клиент құрылғысына Kaspersky Security Center Басқару серверін орнатыңыз.

3. **Басқару серверлерінің иерархиясын жасау**

   Егер сіз қосалқы Басқару серверін демилитаризацияланған аймаққа орналастырсаңыз, қосалқы Басқару сервері негізгі Басқару серверінен қосылымды қабылдауы керек. Негізгі Сервер 13000-порт арқылы қосалқы Серверге қосылуы үшін жаңа Басқару серверін қосалқы Сервер ретінде қосыңыз. Серверлерді иерархияға біріктіру кезінде екі Сервердің 13299-порты қолжетімді болуы керек. Kaspersky Security Center Web Console бағдарламасы Басқару серверіне 13299-порт арқылы қосылады.

4. **Автономды басқарылатын құрылғыларды қосалқы Басқару серверіне қосу**

   Автономды құрылғыларды Басқару сервері мен негізгі желіде орналасқан басқарылатын құрылғылар арасында байланыс орнатылатындай демилитаризацияланған аймақтағы Басқару серверіне қосуға болады. Автономды құрылғылар қосылымды 13000 порты арқылы іске қосады.

Автономды құрылғыларды қосу туралы

Әрқашан негізгі желіден тыс кейбір басқарылатын құрылғыларды (мысалы, компанияның аймақтық филиалдарындағы компьютерлер; әртүрлі сату орындарында орнатылған дүңгіршектер, банкоматтар және терминалдар; қызметкерлердің үй кеңселеріндегі компьютерлер) басқару серверіне тікелей қосу мүмкін емес. Кейбір құрылғылар кейде желінің периметрінен асып кетеді (мысалы, аймақтық филиалдарға немесе клиенттің кеңсесіне баратын пайдаланушылардың ноутбуктері).

Сіз әлі де кеңседен тыс құрылғылардың қорғанысын қадағалап, басқаруыңыз керек – олардың қорғаныс күйі туралы өзекті ақпарат алу және олардағы қауіпсіздік бағдарламаларын жаңартып отыру. Бұл, мысалы, мұндай құрылғы негізгі желіден алшақ жерде бұзылатын болса, ол негізгі желіге қосылғаннан кейін бірден қауіп тарататын платформаға айналуы мүмкін болғандықтан қажет. Автономды құрылғыларды Басқару серверіне қосу үшін келесі екі тәсілді қолдануға болады:

- Демилитаризацияланған аймақтағы (DMZ) қосылымдар шлюзі

  Деректер трафигі схемасын қараңыз: Жергілікті желі (LAN) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар; қосылым шлюзін қолдану.

- Демилитаризацияланған аймақтағы (DMZ) Басқару сервері

  Деректер трафигі схемасын қараңыз: Демилитаризацияланған аймақтың (DMZ) ішіндегі Басқару сервері, интернеттегі басқарылатын құрылғылар.

Демилитаризацияланған аймақтағы қосылымдар шлюзі

Автономды құрылғыларды Басқару серверіне қосудың ұсынылған тәсілі – ұйым желісінде демилитаризацияланған аймақты құру және демилитаризацияланған аймақта қосылым шлюзін орнату. Сыртқы құрылғылар қосылым шлюзіне қосылады, ал желі ішіндегі Басқару сервері құрылғыларға қосылым шлюзі арқылы қосылымды бастайды.

Басқасымен салыстырғанда, бұл ең қауіпсіз болып есептеледі:

- Басқару серверіне сырттан қатынасуды ашудың қажеті жоқ.
- Бұзылған қосылым шлюзі желілік құрылғылардың қауіпсіздігіне үлкен қауіп төндірмейді. Қосылым шлюзі ештеңені басқармайды немесе ешқандай қосылымды орнатпайды.

Бұдан бөлек, қосылым шлюзі көп аппараттық ресурсты қажет етпейді.

Алайда, бұл тәсіл аса күрделі конфигурациялау процесіне ие:

- Құрылғы демилитаризацияланған аймақта қосылым шлюзі рөлін атқаруы үшін сізге Желілік агент орнатып, оны Басқару серверіне ерекше түрде қосу керек.
- Жағдайлар үшін Басқару серверіне бірдей қосылым мекенжайын пайдалана алмайсыз. Периметрдің сыртында сізге басқа мекенжайды (қосылым шлюзінің мекенжайын) ғана емес, сонымен қатар басқа қосылым режимін де қолдану қажет болады: қосылым шлюзі арқылы.
- Сондай-ақ, әртүрлі орындардағы ноутбуктер үшін әртүрлі қосылым параметрлерін анықтау қажет.

Бұрын конфигурацияланған желіге қосылым шлюзін қосу үшін:

1. Желілік агентті қосылым шлюзі режимінде орнатыңыз.
2. Жаңадан қосылған қосылым шлюзіне қосқыңыз келетін құрылғыларда Желілік агентті қайта орнатыңыз.

Демилитаризацияланған аймақтағы (DMZ) Басқару сервері

Тағы бір тәсіл – демилитаризацияланған аймақта бірыңғай Басқару серверін орнату.

Бұл конфигурацияның қауіпсіздігі, бірінші тәсілдің конфигурациясына қарағанда төмен. Бұл жағдайда, сыртқы ноутбуктерді басқару үшін Басқару сервері интернеттен кез келген мекенжайдан қосылымдарды қабылдауы керек. Басқару сервері ішкі желідегі барлық құрылғыларды тек демилитаризацияланған аймақтан басқарады. Сондықтан, мұндай оқиғаның ықтималдығы төмен болғанына қарамастан, бұзылған Сервер үлкен зиян келтіруі мүмкін.

Демилитаризацияланған аймақтағы Басқару сервері ішкі желі құрылғыларын басқара алмаса, қауіп айтарлықтай төмендейді. Мұндай конфигурацияны, мысалы, провайдер клиенттердің құрылғыларын басқару үшін қолдана алады.

Бұл тәсілді келесі жағдайларда қолдануға болады:

- Басқару серверін орнатумен және конфигурациялаумен таныс болсаңыз және қосылым шлюзін орнату мен конфигурациялаудың басқа процедурасын орындағыңыз келмесе.
- Егер сізге көптеген құрылғыларды басқару қажет болса. Басқару сервері басқара алатын құрылғылардың ең көп саны – 100 000 құрылғы, қосылым шлюзі 10 000 құрылғыға дейін қолдау көрсете алады.

Бұл шешімнің кейбір қиындықтары да бар:

- Басқару сервері көбірек аппараттық ресурстарды және басқа дерекқорды қажет етеді.
- Құрылғылар туралы ақпарат байланысты емес екі дерекқорда сақталады (желі ішіндегі Басқару сервері үшін және екіншісі демилитаризацияланған аймақта), бұл болса бақылауды қиындатады.
- Барлық құрылғыларды басқару үшін Басқару сервері иерархияға біріктірілуі керек, бұл болса бақылау мен басқаруды қиындатады. Қосалқы Басқару серверінің үлгісі басқару топтарының ықтимал құрылымдарына шектеулер қояды. Қосалқы басқару серверіне қандай тапсырмалар мен саясаттарды және қалай кеңейту керектігін шешуіңіз керек.
- Сыртқы құрылғыларды демилитаризацияланған аймақта Басқару сервері пайдалану үшін және негізгі Басқару серверін ішкі жағынан пайдалану үшін конфигурациялау шлюз арқылы қосылымды конфигурациялаудан оңай емес.
- Қауіпсіздіктің жоғары тәуекелдері. Бұзылған Басқару сервері басқарылатын ноутбуктерді бұзуды жеңілдетеді. Егер бұл орын алса, хакерлер жергілікті желіге шабуылды жалғастыру үшін ноутбуктердің біреуі корпоративті желіге оралғанша күтуі керек.

Сыртқы компьютер құрылғыларын басқару серверіне қосу

Әрқашан негізгі желіден тыс компьютер құрылғыларын (мысалы, компанияның аймақтық филиалдарындағы компьютерлер; әртүрлі сату орындарында орнатылған дүңгіршектер, банкоматтар және терминалдар; қызметкерлердің үй кеңселеріндегі компьютерлер) басқару серверіне тікелей қосу мүмкін емес. Олар Басқару серверіне демилитаризацияланған аймақта (DMZ) орнатылған қосылым шлюзі арқылы қосылуы керек. Бұл конфигурация осы құрылғыларға желілік агент орнатылған кезде орындалады.

Сыртқы компьютер құрылғыларын басқару серверіне қосу үшін:

1. Желілік агенттің орнату пакетін жасау.
2. Жасалған орнату пакетінің сипаттарын ашыңыз, **Параметрлер** → **Кеңейтілген** бөліміне өтіңіз және **Басқару серверіне байланыс шлюзі арқылы қосылу** параметрін ашыңыз.

   Басқару серверіне байланыс шлюзі арқылы қосылу параметрі **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** параметрімен үйлеспейді. Сіз бұл параметрлердің екеуін де бір уақытта қоса алмайсыз.

3. **Қосылым шлюзінің мекенжайы** өрісінде қосылым шлюзі мекенжайын көрсетіңіз.

   Егер қосылым шлюзі Network Address Translation (NAT) артында орналасқан болса және өзінің жалпыға ортақ мекенжайы болмаса, қосылымдарды жалпыға ортақ мекенжайдан қосылым шлюзінің ішкі мекенжайына бағыттау үшін NAT шлюз ережесін конфигурациялаңыз.

4. Жасалған орнату пакеті негізінде Жеке орнату пакетін жасаңыз.
5. Жеке орнату пакетін мақсатты құрылғыларға электронды түрде немесе алынбалы жетекте жеткізіңіз.
6. Жеке орнату пакетіндегі Желілік агентті орнатыңыз.

Басқару серверіне сыртқы компьютер құрылғылары қосылған.

Автономды пайдаланушыларға арналған қосылым профильдері туралы

Ноутбуктерді (бұдан әрі - "құрылғылар") пайдаланатын автономды пайдаланушылар жұмыс істеген кезде, құрылғының желідегі ағымдағы жайғасымына байланысты Басқару серверіне қосылу тәсілін өзгерту немесе Басқару серверлері арасында ауысу қажет болуы мүмкін.

Қосылым профильдеріне тек Windows және macOS басқаратын құрылғылар үшін ғана қолдау көрсетіледі.

Бір Басқару серверінің әртүрлі мекенжайларын пайдалану

Желілік агенті орнатылған құрылғылар әртүрлі уақыт аралығында ұйымның ішкі желісінен де, интернеттен де Басқару серверіне де қосыла алады. Бұл жағдайда, Желілік агент Басқару серверіне қосылу үшін әртүрлі мекенжайларды қолдануы қажет болуы мүмкін: интернеттен қосылған кезде Сервердің сыртқы мекенжайы және ішкі желіден қосылған кезде Сервердің ішкі мекенжайы.

Бұл үшін, Желілік агент саясатының сипаттарында интернеттен Басқару серверіне қосылу үшін профиль қосыңыз (**Бағдарлама параметрлері** → **Қосылым мүмкіндігі** → **Байланыс профильдері** → **Басқару серверіне қосылу профильдері** бөлімінде). Профиль жасау терезесінде **Тек жаңартуларды алу үшін пайдалану** параметрін өшіріңіз және **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау** параметрі таңдалғанына көз жеткізіңіз. Егер қосылым шлюзі Басқару серверіне қатынасу үшін пайдаланылса (мысалы, Интернеттен қатынасу: Желілік агент демилитаризацияланған аймақтағы қосылым шлюзі ретінде бөлімінде сипатталған Kaspersky Security Center конфигурациясында), қосылым профилінде тиісті өрістегі қосылым шлюзінің мекенжайы көрсетілуі керек.

Ағымдағы желіге байланысты Басқару серверлері арасында ауысу

Егер ұйымда әртүрлі Басқару серверлері бар бірнеше кеңселер болса және олардың арасында Желілік агенті орнатылған құрылғылардың бір бөлігі жылжытылса, онда Желілік агент құрылғы орналасқан кеңсенің жергілікті желісін Басқару серверіне қосылуы керек.

Бұл жағдайда, Желілік агент саясатының сипаттарында бастапқы үйдегі Басқару сервері орналасқан үйдегі кеңсені қоспағанда, әрбір кеңсе үшін Басқару серверіне қосылу профилін жасаңыз. Қосылым профильдерінде тиісті Басқару серверлерінің мекенжайларын көрсетіңіз және **Тек жаңартуларды алу үшін пайдалану** параметрін қосыңыз (немесе өшіріңіз):

- Желілік агент үйдегі Басқару серверімен синхрондауды қажет етсе, ал жергілікті Сервер тек жаңартуларды жүктеу үшін пайдаланылса, параметрді таңдаңыз;
- Желілік агент жергілікті Басқару сервері тарапынан толығымен басқарылуы қажет болса, параметрді өшіріңіз.

Әрі қарай, сіз жасалған профильдерге ауысу шарттарын конфигурациялауыңыз керек: "үйдегі кеңсені" қоспағанда, кеңселердің әрқайсысы үшін кемінде бір шарт. Мұндай шарттардың әрқайсысының мәні кеңселердің біріне тән бөлшектерді желілік ортада табуға негізделеді. Егер шарт шындыққа айналса, тиісті профиль белсендіріледі. Егер шарттардың ешқайсысы дұрыс болмаса, Желілік агент үйдегі Басқару серверіне ауысады.

Автономды пайдаланушылар үшін қосылым профилін жасау

Желілік агент профилін Басқару серверіне қосу тек Windows және macOS операциялық жүйесі басқаратын құрылғылар үшін ғана қолжетімді.

Желілік агентті автономды пайдаланушыларға арналған Басқару серверіне қосу профилін жасау үшін:

1. Егер сіз басқарылатын құрылғылар тобы үшін қосылым профилін жасағыңыз келсе, сол топтың Желілік агентінің саясатын ашыңыз. Бұл үшін келесі әрекеттерді орындаңыз:
   a. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
   b. Сілтеме арқылы ағымдағы жолға өтіңіз.
   c. Ашылған терезеде қажетті басқару тобын таңдаңыз.
      Осыдан кейін, ағымдағы жол өзгереді.
   d. Басқарылатын құрылғылар тобы үшін Желілік агент саясатын қосыңыз. Егер сіз оны әлдеқашан жасаған болсаңыз, саясат сипаттарын ашу үшін Желілік агент саясатының атауын басыңыз.
2. Егер сіз белгілі бір басқарылатын құрылғы үшін қосылым профилін жасағыңыз келсе, келесі әрекеттерді орындаңыз:
   a. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
   b. Қажетті басқарылатын құрылғының атауын басыңыз.

c. Ашылған басқарылатын құрылғы сипаттары терезесінде **Бағдарламалар** қойыншасына өтіңіз.

d. Тек таңдалған басқарылатын құрылғы қолданылатын Желілік агент саясатының атауын басыңыз.

3. Ашылған сипаттар терезесінде **Бағдарлама параметрлері → Қосылым мүмкіндігі → Байланыс профильдері бөліміне өтіңіз.**

4. **Басқару серверіне қосылу профильдері** бөлімінде **Қосу** түймесін басыңыз.

   Әдепкі бойынша, қосылым профильдері тізімі <Офлайн-режим> және <Үйдегі Басқару сервері> профильдерін қамтиды. Профильдер өзгерту және жою үшін қолжетімді емес.

   <Офлайн-режим> профилінде қосылуға арналған Сервер көрсетілмейді. Осы профильге өту кезінде, Желілік агент қандай да бір Серверге қосылуға тырыспайды, ал клиент құрылғыларында орнатылған бағдарламалар болса автономды пайдаланушыларға арналған саясаттарды қолданады. <Офлайн-режим> профилі құрылғыны желіден ажырату шарттарында қолданылады.

   <Үйдегі Басқару сервері> профилінде, Желілік агентті орнату кезінде белгіленген қосылуға арналған Сервер көрсетілген. <Үйдегі Басқару сервері> профилі, басқа желіде жұмыс істеген құрылғы қайтадан үйдегі Басқару серверіне қосылатын шарттарда қолданылады.

5. Ашылған **Профильді конфигурациялау** терезесінде қосылым профилінің параметрлерін конфигурациялаңыз:

   - **Профиль атауы**

     Енгізу өрісінде қосылым профилінің атауын қарауға немесе өзгертуге болады.

   - **Басқару серверінің мекенжайы**

     Профильді белсендіру кезінде клиент құрылғысы қосылуы тиісті Басқару серверінің мекенжайы.

   - **Порт нөмірі**

     Қосылым орындалатын порт нөмірі.

   - **SSL порты**

     SSL протоколының көмегімен қосылым орындалатын порт нөмірі.

   - **SSL байланысын пайдалану**

     Бұл параметр қосулы болса, қосылым қорғалған порт арқылы орындалатын болады (SSL протоколының көмегімен).

     Әдепкі бойынша, параметр қосулы. Сіздің қосылымыңыз қауіпсіз болып қала беруі үшін, бұл параметрді өшірмеу ұсынылады.

   - Интернетке қосу үшін прокси-серверді қолдану керек болса, **Прокси-серверді пайдалану** параметрін таңдаңыз. Параметр таңдалған болса, параметрлерді енгізу өрістері қолжетімді болады. Прокси-серверге қосылудың келесі параметрлерін конфигурациялаңыз:

     - **Мекенжай**

       Kaspersky Security Center-ді интернетке қосу үшін прокси-сервер мекенжайы.

     - **Порт нөмірі**

       Kaspersky Security Center прокси-қосылымы орнатылатын порт нөмірі.

- **Прокси-сервердегі түпнұсқалық растама**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

- **Пайдаланушы аты**

  Прокси-серверге қосылатын пайдаланушы есептік жазбасы (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

- **Құпиясөз**

  Прокси-серверге қосылуға мүмкіндік беретін пайдаланушы құпиясөзі (**Прокси-сервердегі түпнұсқалық растама** жалаушасы қойылған болса, өріс қолжетімді болады).

  Енгізілген құпиясөзді қарау үшін, **Көрсету** түймесін басып, оны қажетті уақыт бойы ұстап тұрыңыз.

- **Қосылым шлюзінің мекенжайы**

  Клиент құрылғыларын Басқару серверіне қосатын шлюз мекенжайы.

- **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу**

  Қосылу кезінде клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясаттардың профильдерін және Басқару сервері қолжетімді болмаса, автономды пайдаланушыларға арналған саясаттардың профильдерін қолдануы үшін осы жалаушаны қойыңыз. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, бағдарламалар белсенді саясаттарды қолданатын болады.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Тек жаңартуларды алу үшін пайдалану**

  Бұл параметр қосулы болса, профиль клиент құрылғысында орнатылған бағдарламалар жаңартуларды жүктеп алған кезде ғана қолданылатын болады. Қалған операциялар үшін Басқару серверіне қосылу Желілік агентті орнату кезінде белгіленген бастапқы қосылу параметрлерімен орындалатын болады.

  Әдепкі бойынша, параметр қосулы.

- **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау**

  Бұл параметр қосулы болса, Желілік агент профильдің сипаттарында көрсетілген параметрлерді қолдана отырып, Басқару серверіне қосылады.

  Бұл параметр өшірулі болса, Желілік агент орнату кезінде көрсетілген бастапқы параметрлерді қолдана отырып, Серверге қосылады.

  Тек жаңартуларды алу үшін пайдалану параметрі таңдалса, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

Нәтижесінде, Желілік агентті автономды пайдаланушыларға арналған Басқару серверіне қосу профилі жасалады. Желілік агентті осы профиль арқылы Серверге қосқан кезде, клиент құрылғысында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясаттарды немесе автономды пайдаланушыларға арналған саясаттарды қолданатын болады.

Желілік агентті басқа Басқару серверіне ауыстырып қосу туралы

Kaspersky Security Center-де, желінің келесі сипаттамалары өзгерген кезде клиент құрылғысының Желілік агентін басқа Басқару серверіне ауыстырып қосу мүмкіндігі көзделген:

- **DHCP сервері мекенжайына арналған шарт** – желідегі DHCP (Dynamic Host Configuration Protocol) серверінің IP мекенжайын өзгерту.
- **Әдепкі қосылым шлюзінің мекенжайына арналған шарт** – желінің негізгі шлюзін өзгерту.
- **DNS доменіне арналған шарт** – ішкі желінің DNS суффиксін өзгерту.
- **DNS сервері мекенжайына арналған шарт** – желідегі DNS серверінің IP мекенжайын өзгерту.
- **WINS сервері мекенжайына арналған шарт** – желідегі WINS серверінің IP мекенжайын өзгерту. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.
- **Атау шешіміне арналған шарт** – клиент құрылғысында NetBIOS атауы немесе DNS атауы өзгерді.
- **Қосалқы желіге арналған шарт** – ішкі желі маскасы мен мекенжайын өзгерту.
- **Windows доменінің қолжетімділігіне арналған шарт** – клиент құрылғысы қосылып тұрған Windows доменінің күйін өзгерту. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.
- **SSL қосылым мекенжайының қолжетімділігіне арналған шарт** – клиент құрылғысы көрсетілген сервермен (атауы:порты) SSL қосылымын орната алады немесе орната алмайды (сіз таңдаған параметрге байланысты). Қосылым үшін жоғары жүктемені және жиі желілік агент сұрауларын өңдей алатын бағдарламалық жасақтамасы бар арнайы серверді пайдалану керек. Басқару серверінің портын көрсетпеңіз. Әрбір Сервер үшін сіз SSL сертификатын қосымша түрде көрсете аласыз. Бұл жағдайда желілік агент SSL қосылымының мүмкіндігін тексерумен қатар, басқару серверінің сертификатын тексереді. Сертификаттар сай келмесе, қосылым орнатылмайды.

Бұл функцияға тек Windows немесе macOS басқаратын құрылғыларға орнатылған Желілік агенттер үшін қолдау көрсетіледі.

Желілік агентті Серверге қосудың бастапқы параметрлері Желілік агентті орнату кезінде белгіленеді. Алдағыда, Желілік агентті басқа Басқару серверлеріне ауыстырып қосу ережелері қалыптастырылған болса, Агент желі сипаттамаларының өзгертілуіне келесідей жауап қайтарады:

- Егер желінің сипаттамалары қалыптастырылған ережелердің ешбіріне сай келмесе, онда Желілік агент осы ережеде көрсетілген Басқару серверіне қосылады. Бұл ережемен белгіленген болса, клиент құрылғыларына орнатылған бағдарламалар автономды пайдаланушыларға арналған саясаттарға өтеді.
- Ережелердің ешбірі орындалмай жатса, онда Желілік агент орнату кезінде белгіленген Басқару серверіне қосылу бастапқы параметрлеріне қайта оралады. Клиент құрылғыларында орнатылған бағдарламалар белсенді саясаттарға қайта оралады.
- Басқару сервері қолжетімді болмаса, онда Желілік агент автономды пайдаланушыларға арналған саясаттарды қолданады.

Желілік агент, **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу** параметрі Желілік агент саясатының параметрлерінде қосылған болса ғана автономды пайдаланушыларға арналған саясатқа ауысып қосылады.

Желілік агентті Басқару серверіне қосу параметрлері қосылым профилінде сақталады. Қосылым профилінде сіз клиент құрылғыларын автономды пайдаланушыларға арналған саясаттарға көшіру ережелерін жасай аласыз, сондай-ақ профильді жаңартуларды жүктеп алу үшін қолданылатындай етіп конфигурациялай аласыз.

Желілік агентті желілік орналасу бойынша ауыстырып қосу ережесін жасау

Желілік агентті ауыстырып қосу тек Windows және macOS операциялық жүйесі басқаратын құрылғылар үшін ғана қолжетімді.

Желінің сипаттамаларын өзгерту кезінде Желілік агентті бір Басқару серверінен басқасына ауыстырып қосуға арналған ережені жасау үшін:

1. Егер сіз басқарылатын құрылғылар тобы үшін ереже жасағыңыз келсе, сол топтың Желілік агентінің саясатын ашыңыз. Бұл үшін келесі әрекеттерді орындаңыз:

   a. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

   b. Сілтеме арқылы ағымдағы жолға өтіңіз.

   c. Ашылған терезеде қажетті басқару тобын таңдаңыз.

      Осыдан кейін, ағымдағы жол өзгереді.

   d. Басқарылатын құрылғылар тобы үшін Желілік агент саясатын қосыңыз. Егер сіз оны әлдеқашан жасаған болсаңыз, саясат сипаттарын ашу үшін Желілік агент саясатының атауын басыңыз.

2. Егер сіз белгілі бір басқарылатын құрылғы үшін ереже жасағыңыз келсе, келесі әрекеттерді орындаңыз:

   a. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   b. Қажетті басқарылатын құрылғының атауын басыңыз.

   c. Ашылған басқарылатын құрылғы сипаттары терезесінде **Бағдарламалар** қойыншасына өтіңіз.

   d. Тек таңдалған басқарылатын құрылғы қолданылатын Желілік агент саясатының атауын басыңыз.

3. Ашылған сипаттар терезесінде **Бағдарлама параметрлері** → **Қосылым мүмкіндігі** → **Байланыс профильдері бөліміне өтіңіз.**

4. **Желілік орналасудың параметрлері** бөлімінде **Қосу** түймесін басыңыз.

5. Ашылған сипаттар терезесінде желілік орналасудың сипаттамасын және ауысу ережесін конфигурациялаңыз. Желілік орналасудың сипаттамасының келесі параметрлерін конфигурациялаңыз:

   - **Сипаттама**

     Желілік орналасудың сипаттамасының атауы 255 таңбадан артық болуы және арнайы таңбаларды ("*<>? \/:|) қамтуы мүмкін емес.

   - **Қосылу профилін пайдалану**

     Ашылатын тізімнен Желілік агентті Басқару серверіне қосу профилін таңдауға болады. Профиль желілік орналасудың сипаттамасының шарттарын орындау кезінде қолданылады. Қосылым профилі, Желілік агентті Басқару серверіне қосу параметрлерін қамтиды және клиент құрылғыларын автономды пайдаланушыларға арналған саясаттарға көшіруді айқындайды. Профиль тек жаңартуларды жүктеу үшін ғана қолданылады.

   - **Сипаттама белсенді**

     Жаңа желілік орналасу сипаттамасын пайдалануды қосу үшін осы жалаушаны қойыңыз.

6. Желілік агентті ауыстыру ережесінің шарттарын таңдаңыз:

   - **DHCP сервері мекенжайына арналған шарт** – желідегі DHCP (Dynamic Host Configuration Protocol) серверінің IP мекенжайын өзгерту.

   - **Әдепкі қосылым шлюзінің мекенжайына арналған шарт** – желінің негізгі шлюзін өзгерту.

   - **DNS доменіне арналған шарт** – ішкі желінің DNS суффиксін өзгерту.

   - **DNS сервері мекенжайына арналған шарт** – желідегі DNS серверінің IP мекенжайын өзгерту.

   - **WINS сервері мекенжайына арналған шарт** – желідегі WINS серверінің IP мекенжайын өзгерту. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.

   - **Атау шешіміне арналған шарт** – клиент құрылғысында NetBIOS атауы немесе DNS атауы өзгерді.

   - **Қосалқы желіге арналған шарт** – ішкі желі маскасы мен мекенжайын өзгерту.

- **Windows доменінің қолжетімділігіне арналған шарт** – клиент құрылғысы қосылып тұрған Windows доменінің күйін өзгерту. Бұл параметр Windows операциялық жүйелері орнатылған құрылғылар үшін ғана қолжетімді.

- **SSL қосылым мекенжайының қолжетімділігіне арналған шарт** – клиент құрылғысы Сервермен (атауы:порты) SSL қосылымын орната алады немесе орната алмайды (сіз таңдаған параметрге байланысты). Әрбір Сервер үшін сіз SSL сертификатын қосымша түрде көрсете аласыз. Бұл жағдайда, Желілік агент SSL қосылымының мүмкіндігін тексерумен қатар, Басқару серверінің сертификатын тексереді. Сертификаттар сай келмесе, қосылым орнатылмайды.

Ереженің шарттары AND логикалық операторын қолданумен бірге біріктіріледі. Желілік орналасудың сипаттамасы бойынша ауысу ережесі іске қосылуы үшін, ереженің барлық ауысу шарттары орындалуы тиіс.

7. Шарттар бөлімінде Желілік агентті басқа Басқару серверіне қашан ауыстыру қажет екенін көрсетіңіз. Бұл үшін **Қосу** түймесін басыңыз және шарттың мәнін белгілеңіз.

   Тізімнің кемінде бір мәніне сәйкес болса параметрі әдепкі бойынша қосулы. Егер сіз шарттың барлық көрсетілген мәндермен орындалуын қаласаңыз, бұл параметрді өшіруге болады.

8. Өзгерістерді сақтаңыз.

Нәтижесінде, желілік орналасудың сипаттамасы бойынша ауыстырып қосу ережесі жасалып, оның шарттарын орындау кезінде Желілік агент Басқару серверіне қосылу үшін сипаттамада көрсетілген қосылым профилін қолданатын болады.

Қорғанысты орналастыру шебері

Kaspersky бағдарламаларын орнату үшін қорғанысты орналастыру шеберін пайдалануға болады. Қорғанысты орналастыру шебері бағдарламаларды арнайы жасалған орнату пакеттері арқылы және тікелей дистрибутивтерден қашықтан орнатуға мүмкіндік береді.

Қорғанысты орналастыру шебері келесі әрекеттерді орындайды:

- Бағдарламаны орнату үшін орнату пакетін жүктейді (егер ол бұрын жасалмаған болса). Орнату пакеті осы жолда орналасқан: **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері**. Бағдарламаны кейінірек орнату үшін осы орнату пакетін пайдалануға болады.

- Құрылғылар жиынтығы немесе басқару тобы үшін қашықтан орнату тапсырмасын жасайды және іске қосады. Құрылған қашықтан орнату тапсырмасы **Тапсырмалар** бөлімінде сақталады. Бұл тапсырманы кейінірек қолмен іске қосуға болады. Тапсырма түрі – **Бағдарламаны қашықтан орнату**.

SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

1-қадам. Қорғанысты орналастыру шеберін іске қосу

Қорғанысты орналастыру шеберін қолмен іске қосу үшін,

Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Қорғанысты орналастыру шебері** бөліміне өтіңіз.

Қорғанысты орналастыру шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2-қадам. Орнату пакетін таңдау

Орнатқыңыз келетін бағдарламаның орнату пакетін таңдаңыз.

Қажетті бағдарламаның орнату пакеті тізімде болмаса, **Қосу** түймесін басып, тізімнен бағдарламаны таңдаңыз.

3-қадам. Кілт файлын немесе белсендіру кодын тарату тәсілін таңдау

Кілт файлын немесе белсендіру кодын тарату тәсілін таңдаңыз:

- **Лицензиялық кілтті орнату пакетіне қоспау**

  Егер бұл нұсқа таңдалса, кілт автоматты түрде сәйкес келетін құрылғыларға таратылады:
  - егер кілттің сипаттарында автоматты түрде тарату конфигурацияланған болса;
  - **Кілтті қосу** тапсырмасы жасалған болса.

- **Лицензиялық кілтті орнату пакетіне қосу**

  Кілт орнату пакетімен бірге құрылғыларға таралады.

  > Кілтті осылайша тарату ұсынылмайды, өйткені әдепкі бойынша орнату пакетінің қоймасы оқуға ортақ қатынасуға конфигурацияланған.

Егер орнату пакетінде кілт файлы немесе белсендіру коды болса, бұл терезе көрсетіледі, бірақ ол тек лицензиялық кілт туралы ақпаратты қамтиды.

4-қадам. Желілік агенттің нұсқасын таңдау

Желілік агенттен басқа бағдарламаның орнату пакетін таңдаған болсаңыз, бағдарламаны Kaspersky Security Center Басқару серверіне қосу үшін Желілік агентті де орнату қажет.

Желілік агенттің соңғы нұсқасын таңдаңыз.

5-қадам. Құрылғыларды таңдау

Бағдарламаны орнатуды қажет ететін құрылғылардың тізімін көрсетіңіз:

- **Басқарылатын құрылғыларда орнату**

  Егер бұл нұсқа таңдалса, құрылғылар тобы үшін бағдарламаны қашықтан орнату тапсырмасы жасалады.

- **Орнату үшін құрылғыларды таңдау**

  Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

  Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

6-қадам. Қашықтан орнату тапсырмасының параметрлерін орнату

«Қашықтан орнату» тапсырмасы параметрлері терезесінде бағдарламаны қашықтан орнату параметрлерін конфигурациялаңыз.

Орнату пакетін мәжбүрлеп жүктеп алу параметрлер блогында қолданбаны орнату үшін қажетті файлдарды клиент құрылғыларына жеткізу тәсілін таңдаңыз:

- **Желілік агенттің көмегімен**

  Егер бұл параметр қосылса, орнату пакеттерін клиент құрылғыларына жеткізуді клиент құрылғыларына орнатылған Желілік агент жүзеге асырады.

  Егер бұл параметр өшірулі болса, орнату пакеттері клиент құрылғысының операциялық жүйесі құралдарының көмегімен жеткізіледі.

  Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

  Әдепкі бойынша, параметр қосулы.

- **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

  Егер бұл параметр қосылса, орнату пакеттері тарату нүктелері арқылы операциялық жүйенің көмегімен клиент құрылғыларына беріледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл нұсқаны таңдауға болады.

  Желілік агент көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

Әдепкі бойынша, параметр виртуалды Басқару серверінде жасалған қашықтан орнату тапсырмалары үшін қосылған.

> Құрылғыға тағайындалған барлық тарату нүктелері ақаулы болған кезде, құрылғы жаңартуларды (антивирустық дерекқорлар мен патчтарды) және орнату пакеттерін алмайды.

- **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

  Бұл параметр қосылса, файлдар Басқару сервері көмегімен клиент құрылғыларының операциялық жүйесі арқылы клиент құрылғыларына жеткізіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

  Әдепкі бойынша, параметр қосулы.

Қосымша параметрлерді конфигурациялаңыз:

- **Бұрын орнатылып қойған жағдайда, бағдарламаны қайта орнатпау**

  Егер бұл параметр қосылса, таңдалған бағдарлама клиент құрылғысында орнатылған болса, қайта орнатылмайды.

  Егер бұл параметр өшірулі болса, бағдарлама кез келген жағдайда орнатылады.

  Әдепкі бойынша, параметр қосулы.

- **Active Directory топтық саясаттарында бума орнатуды тағайындау**

  Егер бұл параметр қосылса, орнату пакеті Active Directory топтық саясаттары арқылы орнатылады.

  Егер Желілік агенттің орнату пакеті таңдалса, параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

7-қадам. Өшіріп қайта қосуды басқару

Бағдарламаны орнату кезінде операциялық жүйені қайта іске қосу қажет болса, орындалатын әрекетті көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Келесі уақыттан кейін қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

8-қадам. Орнатудың алдында үйлесімді емес бағдарламаларды жою

Бұл қадам, сіз орналастыратын бағдарлама басқа бағдарламалармен үйлесімді болмаса ғана болады.

Kaspersky Security Center бағдарламасы сіз орнатып жатқан бағдарламамен үйлесімді емес бағдарламаларды автоматты түрде жойғанын қаласаңыз, осы параметрді таңдаңыз.

Үйлесімді емес бағдарламалар тізімі көрсетіледі.

Егер бұл параметр таңдалмаса, бағдарлама тек үйлесімді емес бағдарламалары жоқ құрылғыларда орнатылады.

9-қадам. Құрылғыларды басқарылатын құрылғылар қалтасына жылжыту

Желілік агент орнатылғаннан кейін, құрылғыларды басқару тобына жылжыту керек пе екенін көрсетіңіз.

- **Құрылғыларды жылжытпау**

  Құрылғылар тиесілі болып саналатын топтарда қалады. Топтардың ешқайсысына жатпайтын құрылғылар таратылмаған болып қалады.

- **Тағайындалмаған құрылғыларды топқа жылжыту**

  Құрылғылар сіз таңдаған басқару тобына жылжытылады.

Әдепкі бойынша, **Құрылғыларды жылжытпау** нұсқасы таңдалған. Қауіпсіздік тұрғысынан, сіз құрылғыларды қолмен жылжытуды таңдай аласыз.

10-қадам. Құрылғыларға қатынасу үшін есептік жазбаларды таңдау

Қажет болса, қашықтан орнату тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

- **Есептік жазба қажет емес (Желілік агент орнатылды)**

  Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

  Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

- **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

  Егер сіз қашықтан орнату тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда бағдарламаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

  - **Жергілікті есептік жазба**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті есептік жазба** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

    Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

  - **SSH сертификаты**. Бағдарламаны Linux басқаратын клиенттік құрылғыға орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Назар аударыңыз, Kaspersky Security Center, PEM жабық кілттері пішімін қолдайды, бірақ ssh-keygen утилитасы әдепкі бойынша OPENSSH пішіміндегі SSH кілттерін генерациялайды. OPENSSH пішімін Kaspersky Security Center қолдайды. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз. Мысалы:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<пайдаланушының электрондық поштасы>"
```

11-қадам. Орнатуды бастау

Бұл қадамның соңғы қадамы. Осы қадамда **Қашықтан орнату тапсырмасы** сәтті түрде жасалып, конфигурацияланды.

Әдепкі бойынша **Шебердің жұмысы аяқталғаннан кейін тапсырманы іске қосу** нұсқасы таңдалмаған. Осы параметрді таңдасаңыз, шебердің жұмысы аяқталғаннан кейін **Қашықтан орнату тапсырмасы** бірден басталады. Осы параметрді таңдамасаңыз, **Қашықтан орнату тапсырмасы** басталмайды. Бұл тапсырманы кейінірек қолмен іске қосуға болады.

Қорғанысты орналастыру шеберінің соңғы қадамын аяқтау үшін **OK** түймесін басыңыз.

Kaspersky бағдарламаларын Kaspersky Security Center Web Console көмегімен орналастыру

Бұл бөлімде Kaspersky Security Center Web Console көмегімен ұйымыңыздағы клиент құрылғыларында Kaspersky бағдарламаларын қалай орналастыру керектігі сипатталған.

Сценарий: Kaspersky бағдарламаларын Kaspersky Security Center Web Console көмегімен орналастыру

Бұл сценарийде Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалық жасақтамасын орналастыру рәсімі сипатталған. Бағдарламаны жылдам іске қосу шеберін және қорғанысты орналастыру шеберін қолдануға немесе барлық қажетті қадамдарды қолмен орындауға болады.

Келесі бағдарламалар Kaspersky Security Center Web Console көмегімен орналастыру үшін қолжетімді:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Кезеңдер

Kaspersky бағдарламалық жасақтамасын орналастыру келесі кезеңдерден тұрады:

1. **Бағдарламаларды басқару плагинін жүктеу.**

   Бұл кезеңді бағдарламаны жылдам іске қосу шебері өңдейді. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, Kaspersky Endpoint Security for Windows плагинін қолмен жүктеңіз.

   Корпоративті ұялы құрылғыларды басқарғыңыз келсе, Kaspersky Endpoint Security for Android басқару плагиндерін жүктеу және орнату үшін Kaspersky Security for Mobile анықтамасындағы нұсқауларды орындаңыз.

2. **Орнату пакеттерін жүктеу және жасау**

   Бұл кезеңді бағдарламаны жылдам іске қосу шебері өңдейді.

   Бағдарламаны жылдам іске қосу шебері орнату пакетін басқару веб-плагинімен бірге жүктеуге мүмкіндік береді. Шеберді іске қосу кезінде осы параметрді таңдамасаңыз немесе шеберді іске қоспасаңыз, орнату пакетін қолмен жүктеу керек.

   Kaspersky қолданбаларын Kaspersky Security Center көмегімен кейбір құрылғыларда, мысалы, қашықтағы қызметкерлердің құрылғыларында орната алмасаңыз, бағдарламалар үшін автономды орнату пакеттерін жасай аласыз. Kaspersky бағдарламаларын орнату үшін автономды пакеттерді қолдансаңыз, қашықтан орнату тапсырмасын жасау және іске қосу, сондай-ақ Kaspersky Endpoint Security for Windows үшін тапсырмаларды жасау және конфигурациялау қажет емес.

3. **Қашықтан орнату тапсырмасын жасау, конфигурациялау және іске қосу**

   Kaspersky Endpoint Security for Windows үшін, бұл кезең бағдарламаны жылдам іске қосу шебері аяқталғаннан кейін автоматты түрде іске қосылатын қорғанысты орналастыру шеберіне кіреді. Қорғанысты орналастыру шеберін іске қоспаған болсаңыз, осы тапсырманы қолмен жасау және конфигурациялау керек.

   Әртүрлі басқару топтары немесе құрылғылар таңдауы үшін бірнеше қашықтан орнату тапсырмасын қолмен жасауға болады. Осы тапсырмаларда бір бағдарламаның әртүрлі нұсқаларын орналастыруға болады.

   Желідегі барлық құрылғылардың анықталғанына көз жеткізіңіз, содан кейін қашықтан орнату тапсырмасын (немесе тапсырмаларын) іске қосыңыз.

   > Linux негізіндегі активтеріңізге nmap утилитасын орнатыңыз. Бұл утилита Network Location Awareness функциясын қосу үшін қажет.

   > SUSE Linux Enterprise Server 15 операциялық жүйесі бар құрылғыларға Желілік агентті орнатқыңыз келсе, алдымен Желілік агентті орнату үшін insserv-compat пакетін орнатыңыз.

   > Желілік агентті RED OS 7.3.4 не одан кейінгі нұсқадағы немесе MSVSPHERE 9.2 не одан кейінгі нұсқадағы операциялық жүйені қолданатын құрылғыларға орнатқыңыз келсе, желілік агенттің дұрыс жұмыс істеуіне арналған libxcrypt-compat пакетін орнатыңыз.

4. **Басқарылатын бағдарлама үшін тапсырмаларды жасау және конфигурациялау**

   Kaspersky Endpoint Security for Windows *жаңартуларын орнату* тапсырмасы конфигурациялануы тиіс.

Бұл кезең бағдарламаны жылдам іске қосу шеберіне кіреді: тапсырма әдепкі бойынша параметрлермен автоматты түрде жасалады және конфигурацияланады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, осы тапсырманы қолмен жасау және конфигурациялау керек. Бағдарламаны жылдам іске қосу шеберін іске қосқан болсаңыз, онда тапсырманы іске қосу кестесі сіздің талаптарыңызға сай келетініне көз жеткізіңіз. (Әдепкі бойынша, тапсырманы іске қосу уақыты үшін **Қолмен** мәні белгіленген, бірақ сізге осы мәнді өзгерту қажет болуы мүмкін).

Kaspersky басқа бағдарламалары үшін әдепкі бойынша басқа тапсырмалар болуы мүмкін. Кеңейтілген ақпаратты тиісті бағдарламаларға құжаттамадан қараңыз.

Сіз жасаған әрбір тапсырманы іске қосу кестесі сіздің талаптарыңызға сәйкес келетініне көз жеткізіңіз.

5. **Kaspersky Security for Mobile орнату (міндетті емес)**

   Корпоративтік ұялы құрылғыларды басқаруды жоспарласаңыз, Kaspersky Endpoint Security for Android орналастыру туралы ақпарат алу үшін Kaspersky Security for Mobile анықтамасын қараңыз.

6. **Саясаттар жасау**

   Саясатты әрбір бағдарлама үшін қолмен немесе (Kaspersky Endpoint Security for Windows қолдансаңыз) бағдарламаны жылдам іске қосу шебері көмегімен жасаңыз. Саясаттың әдепкі параметрлерін пайдалануға болады; сонымен қатар саясаттың әдепкі параметрлерін қажеттіліктеріңізге сәйкес кез келген уақытта өзгертуге болады.

7. **Нәтижелерді тексеру**

   Орналастырудың сәтті орындалғанына көз жеткізіңіз: әрбір бағдарлама үшін саясаттар мен тапсырмалар жасалған және осы бағдарламалар басқарылатын құрылғыларға орнатылған.

Нәтижелер

Сценарийдің аяқталуы арқасында:

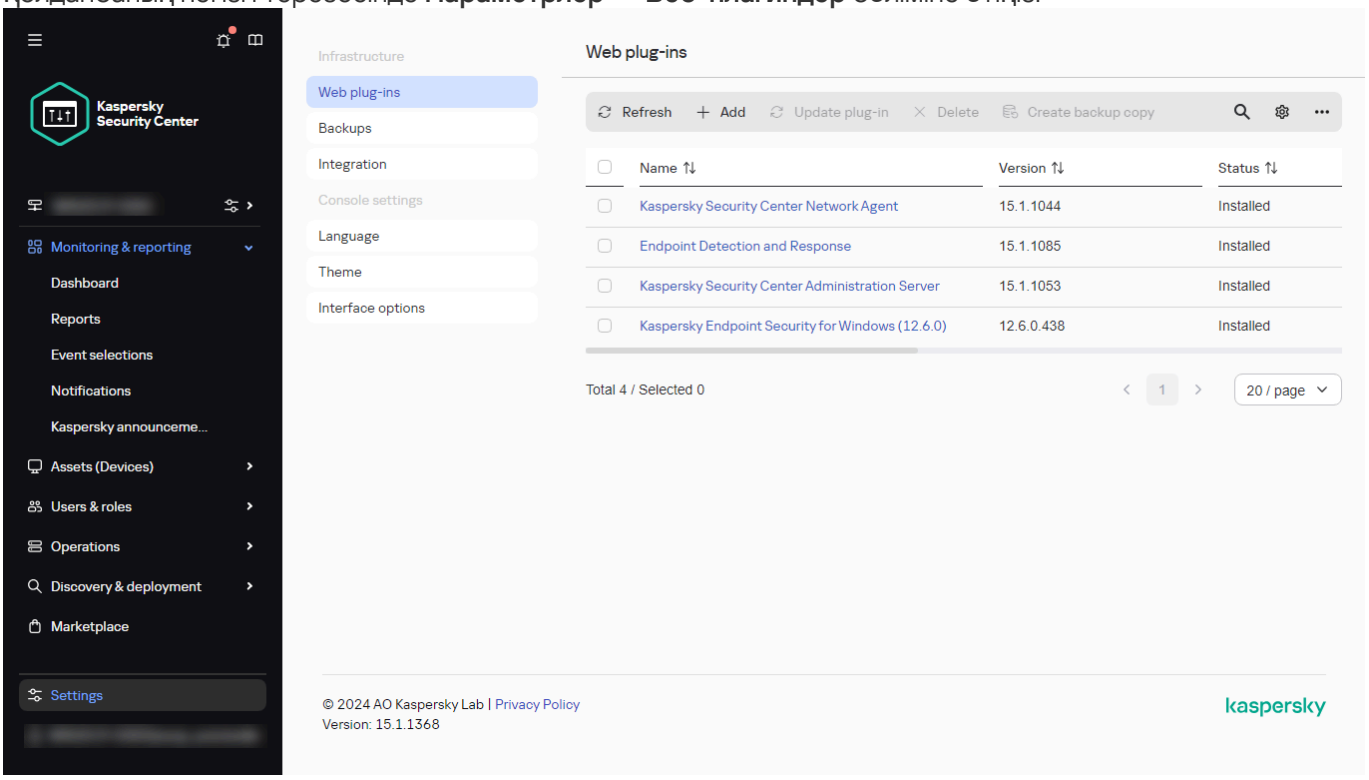
- Таңдалған тапсырмалар үшін барлық қажетті саясаттар мен тапсырмалар жасалады.
- Тапсырмаларды іске қосу кестесі өз талаптарыңызға сай конфигурацияланады.
- Таңдалған клиент құрылғыларында таңдалған бағдарламалар орналастырылған немесе орналастырылуға жоспарланған.

Kaspersky бағдарламаларының плагиндерін жүктеу

Kaspersky Endpoint Security for Windows сияқты Kaspersky бағдарламаларын орналастыру үшін, осы бағдарламаларға арналған басқару плагиндерін жүктеу керек.

Kaspersky бағдарламаларының плагиндерін жүктеу үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.



Орнатылған веб-плагиндердің тізімі

2. Пайда болған терезеде **Қосу** түймесін басыңыз.

   Қолжетімді басқару плагиндері тізімі көрсетіледі.

3. Қолжетімді плагиндер тізімінде жүктеу қажет болған плагин атауын таңдаңыз (мысалы, Kaspersky Endpoint Security 11 for Windows).

   Плагин сипаттамасы бар бет көрсетіледі.

4. Плагин сипаттамасы бетінде **Плагинді орнату** түймесін басыңыз.

5. Орнату аяқталғаннан кейін, **OK** түймесін басыңыз.

Басқару плагині әдепкі бойынша конфигурацияда жүктеледі және басқару плагиндерінің тізімінде пайда болады.

Плагиндерді қосуға және жүктелген плагиндерді файлдан жаңартуға болады. Басқару плагиндері мен басқару веб-плагиндерін Kaspersky Техникалық қолдау қызметі сайтынан жүктеп алуға болады.

Файлдағы плагинді жүктеу немесе жаңарту үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Файлдағы плагинді жүктеу үшін **Файлдан қосу** түймесін басыңыз.
   - Файлдағы плагин үшін жаңартуды жүктеу мақсатымен **Файлдан жаңарту** түймесін басыңыз.

3. Файл мен файл жазуын көрсетіңіз.

4. Көрсетілген файлдарды жүктеңіз.

Басқару плагині файлдан жүктеледі және басқару плагиндерінің тізімінде пайда болады.

Kaspersky бағдарламаларына арналған орнату пакеттерін жүктеп алу және жасау

Басқару сервері интернетке қатынаса алса, сіз Kaspersky веб-серверлерінен Kaspersky бағдарламаларының орнату пакеттерін жасай аласыз.

Kaspersky бағдарламаларына арналған орнату пакеттерін жүктеп алу және жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.

   - Бағдарламаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.

   Сондай-ақ, Kaspersky бағдарламаларына арналған жаңа пакеттер туралы ақпаратты экрандағы хабарландырулар тізімінен көруге болады. Жаңа пакет туралы хабарландырулар болса, хабарландырудың жанындағы сілтеме бойынша қолжетімді орнату пакеттерінің тізіміне өтуге болады.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Kaspersky бағдарламасы үшін орнату пакетін жасаңыз** таңдаңыз.

   Kaspersky веб-серверлерінде қолжетімді орнату пакеттерінің тізімі көрсетіледі. Тізімде тек Kaspersky Security Center бағдарламасының ағымдағы нұсқасымен үйлесімді бағдарламалардың орнату пакеттері бар.

4. Қажетті орнату пакетін, мысалы, Kaspersky Endpoint Security for Windows (11.1.0) нұсқасын таңдаңыз.

   Орнату пакеті туралы ақпараты бар терезе ашылады.

   Қолданыстағы заңдар мен ережелерге сәйкес келсе, сенімді шифрлауды іске асыратын криптографиялық құралдарды қамтитын орнату пакетін жүктеп, пайдалана аласыз. Ұйымыңыздың қажеттіліктері үшін жарамды Kaspersky Endpoint Security for Windows орнату пакетін жүктеп алу үшін ұйымыңыздың клиент құрылғылары орналасқан елдің заңнамасын қараңыз.

5. Ақпаратпен танысып, **Орнату пакетін жүктеп алу және жасау** түймесін басыңыз.

   Дистрибутив пакетін орнату пакетіне түрлендіру мүмкін болмаса, **Орнату пакетін жүктеп алу және жасау** түймесінің орнына **Дистрибутивті жүктеп алу** түймесі көрсетіледі.

   Орнату пакетін Басқару серверіне жүктеп салу басталады. Шебер терезесін жабуға немесе нұсқаулықтың келесі қадамына өтуге болады. Шеберді жапсаңыз, жүктеу процесі фондық режимде жалғасады.

Орнату пакетін жүктеп салу процесін қадағалағыңыз келсе:

a. Бағдарламаның негізгі терезесінде **Операциялар → Қоймалар → Орнату пакеттері → Орындалып жатыр ()** бөліміне өтіңіз.

b. Кестенің **Жүктеп алудың орындалу барысы** және **Жүктеп алу күйі** бағандарында операцияның барысын қадағалаңыз.

Процесс аяқталғаннан кейін, орнату пакеті **Жүктеп алынды** қойыншасындағы тізімге қосылады. Егер жүктеу процесі тоқтап, жүктеу күйі **Түпкі пайдаланушының лицензиялық келісімін қабылдау** болып өзгерсе, орнату пакетінің атауын басып, нұсқаулықтың келесі қадамына өтіңіз.

Таңдалған дистрибутивтегі деректердің өлшемі ағымдағы шекті мәннен асып кетсе, қате туралы хабарлама көрсетіледі. Сіз шекті мәнді өзгерте аласыз және орнату пакетін құруды жалғастыра аласыз.

6. Кейбір Kaspersky бағдарламаларын жүктеу процесі кезінде **Түпкі пайдаланушының лицензиялық келісімін көрсету** түймесі көрсетіледі Осы түйме көрсетілсе:

   a. Лицензиялық келісімін (EULA) оқу үшін **Түпкі пайдаланушының лицензиялық келісімін көрсету** түймесін басыңыз.

   b. Экранда пайда болған Лицензиялық келісімді оқып, **Қабылдау** түймесін басыңыз.

   Лицензиялық келісімді қабылдағаннан кейін, жүктеу жалғасады. **Қабылдамау** түймесін бассаңыз, жүктеу тоқтатылады.

7. Жүктеу аяқталғаннан кейін, **Жабу** түймесін басыңыз.

Таңдалған орнату пакеті, Packages қалтасына салынған Басқару серверінің ортақ қатынас бар қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде көрсетіледі.

Пайдаланушының орнату пакетінің өлшеміне қойылған шектеулерді өзгерту

Таңдаулы орнату пакетін жасау кезінде шығарып алынған деректердің жалпы өлшемі шектеулі. Әдепкі бойынша шектеуі – 1 ГБ.

Егер сіз ағымдағы шектеуден асатын деректерді қамтитын мұрағат файлын жүктеуге тырыссаңыз, қате туралы хабар пайда болады. Үлкен дистрибутивтерден орнату пакеттерін жасау кезінде сізге осы максималды мәнді арттыру қажет болуы мүмкін.

Конфигурацияланатын орнату пакетінің өлшемі үшін максималды мәнді өзгерту үшін:

1. Басқару сервері құрылғысында Басқару серверін орнату үшін пайдаланылған есептік жазбаның астындағы пәрмен жолын іске қосыңыз.

2. Ағымдағы директорияны Kaspersky Security Center орнату қалтасына өзгертіңіз (әдетте бұл <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Басқару серверін орнату түріне байланысты, әкімші артықшылықтары бар келесі пәрмендердің бірін енгізіңіз:

   - Кәдімгі жергілікті орнату:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <байттар_саны>
     ```

   - Ақауларға төзімді Kaspersky Security Center кластеріне орнату:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <байттар_саны> --stp klfoc
     ```

   - Ақауларға төзімді Windows Server кластерін орнату:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <байттар_саны> --stp
     cluster
     ```

   Мұндағы <байттар_саны> – он алтылық немесе ондық пішімдегі байттар саны.

   Мысалы, егер талап етілетін максималды мән 2 ГБ болса, 2147483648 ондық мәнін немесе 0x80000000 он алтылық мәнін көрсетуге болады. Бұл жағдайда, Басқару серверін жергілікті орнату үшін келесі пәрменді пайдалануға болады:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Орнату пакетінің пайдаланушы деректерінің өлшеміне шектеу өзгертілді.

Kaspersky бағдарламалары үшін дистрибутивтерді жүктеу

Kaspersky Security Center Web Console веб-консолінде сіз Kaspersky бағдарламалары үшін дистрибутивті жүктеп алып, сақтай аласыз. Бағдарламаларды қолмен орнатуға арналған дистрибутивтерді Kaspersky Security Center қолданбай пайдалануға болады.

Kaspersky бағдарламаларының дистрибутивін жүктеп алу және сақтау үшін:

1. Басты мәзірде **Операциялар** → **Kaspersky бағдарламалары** → **Бағдарламалардың өзекті нұсқалары** тармағына өтіңіз.

   Қолжетімді дистрибутивтердің, плагиндердің және патчтардың тізімі ашылады. Kaspersky Security Center бағдарламаның ағымдағы нұсқасымен үйлесімді элементтерді ғана көрсетеді.

2. Тізімде жүктегіңіз келетін дистрибутивтің атауын басыңыз.

   Дистрибутив сипаттамасы ашылады.

3. Сипаттамасымен танысып, **Орнату пакетін жүктеп алу және жасау** түймесін басыңыз.

   Дистрибутив орнату пакетіне түрлендіре алмаса, онда **Дистрибутивті жүктеп алу** түймесінің орнына **Орнату пакетін жүктеп алу және жасау** түймесі көрсетіледі.

   Орнату пакетін Басқару серверіне жүктеп салу басталады.

Таңдалған орнату пакеті немесе дистрибутив, **Packages** қалтасына салынған Басқару серверінің ортақ қатынас бар қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде көрсетіледі.

Kaspersky Endpoint Security сәтті орналастырылуын тексеру

Kaspersky бағдарламаларын, мысалы, Kaspersky Endpoint Security бағдарламасын дұрыс орналастырғаныңызға көз жеткізу үшін:

1. Kaspersky Security Center Web Console көмегімен мыналарды тексеріңіз:
   - Kaspersky Endpoint Security және/немесе сіз қолданатын басқа қауіпсіздік бағдарламалары саясаттары;
   - Kaspersky Endpoint Security for Windows тапсырмалары: *Вирустарды жылдам іздеу* және *Жаңартуларды орнату* (Егер сіз Kaspersky Endpoint Security for Windows қолдансаңыз);
   - сіз қолданатын басқа қауіпсіздік бағдарламаларына арналған тапсырмалар.
2. Орнату тағайындалған басқарылатын құрылғыларда мынаған көз жеткізіңіз:
   - Kaspersky Endpoint Security немесе Kaspersky басқа қауіпсіздік бағдарламасы орнатылған;
   - Файл қауіптерінен қорғаныс, Веб-қауіптен қорғаныс және Пошта қауіптерінен қорғаныс параметрлері осы құрылғылар үшін жасалған саясатқа сәйкес келеді;
   - Kaspersky Endpoint Security қызметін қолмен іске қосып, тоқтатуға болады;
   - топтық тапсырмаларды қолмен іске қосуға және тоқтатуға болады.

Автономды орнату пакетін жасау

Сіз және сіздің ұйымыңыздағы құрылғы пайдаланушылары бағдарламаларды құрылғыларға қолмен орнату үшін жеке орнату пакеттерін пайдалана аласыз.

Автономды орнату пакеті, Веб-серверге немесе ортақ қатынасы бар қалтаға орналастыруға, пошта арқылы жіберуге немесе клиент құрылғысына басқа тәсілмен жіберуге болатын орындалатын файл (installer.exe) болып саналады. Қолданбаны Kaspersky Security Center қатысуынсыз орнату үшін клиент құрылғысында алынған файлды жергілікті түрде іске қоса алады. Kaspersky бағдарламалары үшін де, Windows, macOS және Linux үшін үшінші тарап бағдарламалары үшін де жеке орнату пакеттерін жасай аласыз. Үшінші тарап қолданбасына арналған жеке орнату пакетін жасау үшін арнаулы орнату пакетін жасау керек.

Жеке орнату пакетінің авторизацияланбаған тұлғаларға қолжетімді емес екеніне көз жеткізіңіз.

Жеке орнату пакетін жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:
   - Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
   - Бағдарламаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. Орнату пакеттері тізімінен пакетті таңдап, тізімнің үстінде **Орналастыру** түймесін басыңыз.

3. **Автономды пакетті пайдалану** параметрін таңдаңыз.

   Нәтижесінде, автономды орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

4. Таңдалған бағдарламамен бірге Желілік агентті орнату керек болса, **Желілік агентті осы бағдарламамен бірге орнату** параметрі қосылғанына көз жеткізіңіз.

   > Опция автономды орнату пакетін жасайтын қолданбаға байланысты көрсетіледі.

   Әдепкі бойынша, параметр қосулы. Құрылғыда Желілік агенттің орнатылғанына сенімді болмасаңыз, осы параметрді қосу ұсынылады. Желілік агент құрылғыда бұрыннан орнатылған болса, онда Желілік агентпен бірге жеке орнату пакетін орнатқаннан кейін, Желілік агент ең жаңа нұсқасына дейін жаңартылатын болады.

   Осы параметрді өшіретін болсаңыз, Желілік агент құрылғыға орнатылмайды және құрылғы басқарылатын болмайды.

   Егер таңдалған бағдарлама үшін жеке орнату пакеті Басқару серверінде бұрыннан бар болса, шебер бұл туралы хабарды көрсетеді. Бұл жағдайда, келесі әрекеттердің бірін таңдауыңыз керек:

   - **Жеке орнату пакетін жасау**. Қолданбаның жаңа нұсқасы үшін жеке орнату пакетін жасаңыңыз келсе және сіз бұған дейін жасаған қолданбаның алдыңғы нұсқасы үшін жеке орнату пакетін қалдырғыңыз келсе, осы опцияны таңдаңыз. Жаңа жеке орнату пакеті басқа қалтада орналасқан.

   - **Бар жеке орнату пакетін пайдалану**. Бар жеке орнату пакетін пайдалануды қаласаңыз, осы параметрді таңдаңыз. Пакет жасау процесі іске қосылмайды.

   - **Бұрыннан бар жеке орнату пакетін қайта құрастыру**. Дәл осы бағдарлама үшін жеке орнату пакетін тағы да жасағыңыз келсе, осы параметрді таңдаңыз. Жеке орнату пакеті дәл осы қалтада орналастырылады.

5. **Басқарылатын құрылғылар тізіміне жылжыту** параметр **Құрылғыларды жылжытпау** параметрі әдепкі бойынша таңдалған. Желілік агентті орнатқаннан кейін, клиент құрылғысын қандай да бір басқару тобына жылжытқыңыз келмесе, осы параметрді қосулы күйде қалдырыңыз.

   Желілік агентті орнатқаннан кейін, клиент құрылғысын жылжытқыңыз келсе, **Тағайындалмаған құрылғыларды осы топқа жылжыту** параметрін таңдаңыз және клиент құрылғысын жылжытқыңыз келетін басқару тобын көрсетіңіз. Әдепкі бойынша, құрылғылар **Басқарылатын құрылғылар** тобына жылжытылады.

6. Жеке орнату пакетін жасау процесі аяқталғаннан кейін, **Дайын** түймесін басыңыз.

   Жеке орнату пакетін жасау шебері жабылады.

Жеке орнату пакеті жасалып, Басқару серверінің ортақ қатынасы бар қалтасының Pkglnst салынған қалтасына орналастырылған. Орнату пакеттері тізімінің үстінде орналасқан **Автономды пакеттердің тізімін көру** түймесін басып, жеке орнату пакеттері тізімін қарап шыға аласыз.

Жеке орнату пакеттері тізімін қарау

Жеке орнату пакеттерінің тізімін және әрбір жеке орнату пакетінің сипаттарын көруге болады.

Барлық орнату пакеттеріне арналған жеке орнату пакеттерінің тізімін көру үшін:

Автономды пакеттердің тізімін көру түймесін басыңыз.

Тізімдегі жеке орнату пакеттерінің сипаттары келесідей көрсетіледі:

- **Пакет атауы**. Пакетке енгізілген бағдарламаның атауынан және нұсқасынан автоматты түрде жасалатын жеке орнату пакетінің атауы.
- **Бағдарлама атауы**. Жеке орнату пакетіне кіретін бағдарламаның атауы.
- **Бағдарламаның нұсқасы**.
- **Желілік агентті орнату пакетінің атауы**. Параметр тек жеке орнату пакетіне Желілік агент қосылған жағдайда ғана көрсетіледі.
- **Желілік агенттің нұсқасы**. Параметр тек жеке орнату пакетіне Желілік агент қосылған жағдайда ғана көрсетіледі.
- **Өлшемі**. Файл өлшемі (МБ).
- **Топ**. Желілік агент орнатылғаннан кейін клиент құрылғысы жылжытылатын топтың аты.
- **Жасалған күні**. Жеке орнату пакетін құру күні мен уақыты.
- **Өзгертілген**. Жеке орнату пакетін өзгерту күні мен уақыты.
- **Жолы**. Жеке орнату пакеті орналасқан қалтаға толық жол.
- **Веб-мекенжай**. Жеке орнату пакетінің орналасқан веб-мекенжайы.
- **Файл хэші**. Параметр, жеке орнату пакетін үшінші тараптар өзгертпегенін және пайдаланушыда сіз жасаған және пайдаланушыға жіберген бірдей файл бар екенін растау үшін пайдаланылады.

Белгілі бір орнату пакеті үшін жеке орнату пакеттерінің тізімін көру үшін,

тізімнен орнату пакетін таңдап, тізімнің үстінен **Автономды пакеттердің тізімін көру** түймесін басыңыз.

Жеке орнату пакеттерінің тізімінде сіз келесі әрекеттерді орындай аласыз:

- **Жариялау** түймесін пайдаланып, Веб-серверде жеке орнату пакетін жариялау. Жарияланған жеке орнату пакетін, жеке орнату пакетіне сілтеме жіберген пайдаланушыларға жүктеп алуға болады.
- **Жариялауды болдырмау** түймесін басу арқылы Веб-серверде жеке орнату пакетін жариялаудан бас тарту. Жарияланбаған жеке орнату пакетін тек сізге және басқа әкімшілерге жүктеуге болады.
- **Жүктеп алу** түймесін басу арқылы құрылғыға жеке орнату пакетін жүктеп алу.
- **Электрондық пошта арқылы жіберу** түймесін басу арқылы офлайн жеке пакетіне сілтемесі бар электрондық поштаны жіберу.
- **Жою** түймесін басып, жеке орнату пакетін жою.

Пайдаланушы орнату пакетін жасау

Сіз конфигурацияланған орнату пакеттерін пайдалана аласыз:

- клиент құрылғыларына кез келген бағдарламаны (мысалы, мәтіндік редактор) орнатыңыз, мысалы, тапсырма арқылы;
- жеке орнату пакетін жасау.

Пайдаланушы орнату пакеті – бұл файлдар жиынтығы бар қалта. Таңдаулы орнату пакетін жасау көзі – *мұрағаттық файл* болып табылады. Мұрағаттық файлда пайдаланушы орнату пакетіне қосылуы керек файл немесе файлдар бар. Пайдаланушы орнату пакетін жасау кезінде, сіз пәрмен жолының параметрлерін көрсете аласыз, мысалы, бағдарламаны тыныш режимде орнату үшін.

Осалдықтар мен патчтарды басқару функциясы үшін белсенді лицензиялық кілтіңіз болса, сіз тиісті пайдаланушы орнату пакеті үшін әдепкі бойынша орнату параметрлерін түрлендіріп, Kaspersky мамандары ұсынған мәндерді қолдана аласыз. Параметрлер, Kaspersky үшінші тарап өндірушілерінің бағдарламалар дерекқорына тиісті орындалатын файл енгізілген жағдайда ғана конфигурацияланатын орнату пакетін жасау кезінде автоматты түрде түрлендіріледі.

Пайдаланушы орнату пакетін жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:
   - Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
   - Бағдарламаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.
2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Файлдан орнату пакетін жасау** тармағын таңдаңыз.
4. Пакет атауын көрсетіңіз және **Шолу** түймесін басыңыз.

   Орнату пакетін жасау үшін файлды таңдауға болатын Windows стандартты **Ашу** терезесі ашылады.
5. Қолжетімді дискілерде орналасқан мұрағаттық файлды таңдаңыз.

   Сіз ZIP, CAB, TAR немесе TAR.GZ пішіміндегі мұрағаттық файлды жүктей аласыз. SFX (өздігінен шығарылатын мұрағат) файлынан орнату пакетін жасау мүмкін емес.

   Параметрлер пакетті орнату барысында түрлендірілгенін қаласаңыз, **Шебердің жұмысы аяқталғаннан кейін параметрлерді Kaspersky Security Center танитын бағдарламалар үшін ұсынылған мәндерге түрлендіру** жалаушасы қойылғанына көз жеткізіп, **Келесі** түймесін басыңыз.

   Kaspersky Security Center Басқару серверіне файл жүктеле бастайды.

Ұсынылатын орнату параметрлерін қолдануды қосқан болсаңыз, Kaspersky Security Center 15.1 бағдарламасы орындалатын файлдың Kaspersky үшінші тарап бағдарламалары дерекқорына қосылғанын тексереді. Егер тексеру сәтті болса, сіз файлдың танылғандығы туралы хабарландыру аласыз. Параметрлер түрлендірілген және конфигурацияланатын орнату пакеті жасалған. Қосымша әрекеттер қажет емес. Шебер терезесін жабу үшін **Аяқтау** түймесін басыңыз.

6. Файлды таңдаңыз (таңдалған мұрағаттық файлдан алынған файлдар тізімінен) және орындалатын файлдың пәрмен жолының параметрлерін көрсетіңіз.

   Бағдарламаны орнату пакетінен тыныш режимде орнату үшін пәрмен жолының параметрлерін көрсетуге болады. Пәрмен жолының параметрлерін көрсету міндетті емес.

   Орнату пакетін жасау процесі басталады.

   Шебер терезесінде процестің аяқталуы туралы ақпарат көрсетіледі.

   Егер орнату пакеті жасалмаса, тиісті хабарландыру көрсетіледі.

7. Шебер терезесін жабу үшін **Аяқтау** түймесін басыңыз.

Жасалған орнату пакеті Басқару серверінің ортақ қатынасы бар қалтасының Packages салынған қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде пайда болады.

Басқару серверінде қолжетімді орнату пакеттері тізімінде, орнату пакетінің атын басу арқылы, келесі әрекеттерді орындай аласыз:

- Орнату пакетінің келесі сипаттарын қарап шыға аласыз:
  - **Атауы**. Орнату пакетінің атауы.
  - **Көзі**. Бағдарлама өндірушісінің атауы.
  - **Бағдарлама**. Пайдаланушы орнату пакетіне қапталған бағдарламаның атауы.
  - **Нұсқа**. Бағдарлама нұсқасы.
  - **Тіл**. Пайдаланушы орнату пакетіне қапталған бағдарламаның тілі.
  - **Өлшемі (МБ)**. Орнату пакетінің өлшемі.
  - **Операциялық жүйе**. Орнату пакеті арналған операциялық жүйенің түрі.
  - **Жасалған күні**. Орнату пакетін жасау күні.
  - **Өзгертілген**. Орнату пакетін өзгерту күні.
  - **Түрі**. Орнату пакетінің түрі.
- Пакеттің атын және пәрмен жолының параметрлерін өзгертіңіз. Бұл функция тек Kaspersky бағдарламалары негізінде жасалмаған пакеттер үшін қолжетімді.

Егер сіз түрлендіру кезінде пайдаланушы пакетін жасау үшін ұсынылған параметрлер мәндерін белгілеген болсаңыз, пайдаланушы орнату пакетінің сипаттарында **Параметрлер** қойыншасында екі қосымша бөлім пайда болуы мүмкін: **Параметрлер** және **Орнату реті**.

Параметрлер бөлімінде кестеде келтірілген келесі сипаттар бар:

- **Атауы**. Бұл бағанда орнату параметріне тағайындалған атау көрсетіледі.
- **Түрі**. Бұл бағанда орнату параметрі түрі көрсетілген.
- **Мән**. Бұл бағанда, орнату параметрі анықтаған деректер түрі көрсетіледі (логикалық мән, файл жолы, сандық мәні, жолы немесе жол мәні).

Орнату реті бөлімінде, пайдаланушы орнату пакетіне қосылған келесі жаңарту сипаттары сипатталған кесте бар:

- **Атауы**. Жаңарту атауы.
- **Сипаттамасы**. Жаңарту сипаттамасы.
- **Көзі**. Жаңарту көзі, яғни Microsoft немесе басқа үшінші тарап өндірушісі жаңартуды шығарды ма.
- **Түрі**. Жаңарту түрі, яғни жаңарту драйверге немесе бағдарламаға арналған ба.
- **Санаты**. Microsoft жаңартулары үшін көрсетілетін Windows Server Жаңарту қызметтері (WSUS) санаттары (Критикалық жаңартулары, Анықтамалық жаңартулар, Драйверлер, Қосымша құрамдастардың пакеттері, Қауіпсіздік жаңартулары, Қызметтік пакеттер, Құралдар, Жинақтаушы жаңарту пакеттері, Жаңартулар немесе Алдыңғы нұсқалардың жаңартулары).
- **MSRC бойынша маңыздылық деңгейі**. Microsoft Security Response Center (MSRC) анықтаған жаңартудың маңыздылық деңгейі.
- **Маңыздылық деңгейі**. Kaspersky анықтаған жаңартудың маңыздылық деңгейі.
- **Патчтың маңыздылық деңгейі (Kaspersky бағдарламаларының патчтары үшін)**. Kaspersky бағдарламаларына арналған болса, патчтың маңыздылық деңгейі.
- **Мақала**. Жаңарту сипаттамасы бар Білім базасындағы мақаланың идентификаторы.
- **Бюллетень**. Жаңарту сипаттамасы бар қауіпсіздік бюллетені идентификаторы.
- **Орнатуға белгіленбеген**. Орнатуға белгіленбеген күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Орнатуға белгіленген**. Орнатуға белгіленген күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Орнатылуда**. Орнатылуда күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Орнатылған**. Орнатылған күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Сәтсіз аяқталды**. Сәтсіз аяқталды күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Қайта іске қосу керек**. Қайта іске қосу керек күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Тіркелген**. Жаңарту тіркелген күн мен уақыт көрсетіледі.
- **Интерактивті түрде орнатылады**. Жаңартуды орнату кезінде пайдаланушы тәжірибесі қажет пе екені көрсетіледі.
- **Қайтарып алынған**. Жаңарту қайтарып алынғаны күн мен уақыт көрсетіледі.

- **Жаңартуды растау күйі**. Жаңартуды орнатудың расталғаны/расталмағаны көрсетеді.
- **Тексеру**. Жаңартудың ағымдағы шығарылымының нөмірі көрсетіледі.
- **Жаңарту идентификаторы**. Жаңарту идентификаторы көрсетіледі.
- **Бағдарлама нұсқасы**. Бағдарлама жаңартылатын нұсқаның нөмірі көрсетіледі.
- **Ауыстырылып жатқан**. Осы жаңартуды ауыстыра алатын басқа да жаңартулар көрсетіледі.
- **Ауыстыратын**. Осы жаңартумен ауыстыруға болатын басқа да жаңартулар көрсетіледі.
- **Лицензиялық келісімнің шарттарын қабылдау керек** Лицензиялық келісімнің шарттарымен келісімді жаңарту керек пе екені көрсетіледі.
- **Өндіруші**. Жаңарту өндірушісінің аты көрсетіледі.
- **Бағдарламалар тобы**. Жаңарту қатысты болып табылатын бағдарламалар тобының аты көрсетіледі.
- **Бағдарлама**. Жаңарту қатысты болып табылатын бағдарламаның аты көрсетіледі.
- **Тіл**. Жаңартудың локализация тілі көрсетіледі.
- **Орнатуға белгіленбеген (жаңа нұсқа)**. Орнатуға белгіленбеген (жаңа нұсқа) күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Алғышарттарды орнатуды қажет етеді**. Алғышарттарды орнатуды қажет етеді күйі жаңартылғаны/жаңартылмағаны көрсетіледі.
- **Жүктеп алу режимі**. Жаңартуларды жүктеп алу режимі көрсетіледі.
- **Патч болып табылады**. Жаңартудың патч болып табылады ма екені көрсетіледі.
- **Орнатылмаған**. Орнатылмаған күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату

Kaspersky Security Center бағдарламасы сізге Kaspersky бағдарламалары үшін және үшінші тарап бағдарламалары үшін орнату пакеттерін жасауға, сондай-ақ орнату пакеттерін клиент құрылғыларына таратуға және пакеттерден бағдарламалар орнатуға мүмкіндік береді. Негізгі Басқару серверіндегі жүктемені оңтайландыру үшін, орнату пакеттерін қосалқы Басқару серверлеріне таратуға болады. Осыдан кейін, қосалқы Серверлер пакеттерді клиент құрылғыларына жібереді, содан кейін сіз клиент құрылғыларына бағдарламаларды қашықтан орната аласыз.

Орнату пакеттерін қосалқы Басқару серверлеріне тарату үшін:

1. Қосалқы Басқару серверлері негізгі Басқару серверіне қосылғанына көз жеткізіңіз.
2. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

   Тапсырмалар тізімі көрсетіледі.
3. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

4. **Жаңа тапсырма параметрлері** бетінде, **Бағдарлама** ашылмалы тізімінен **Kaspersky Security Center** тармағын таңдаңыз. Содан соң, **Тапсырма түрі** ашылмалы тізімінен **Орнату пакетін тарату** тармағын таңдап, тапсырманың атауын көрсетіңіз.

5. **Тапсырма ауқымы** бетінде тапсырма тағайындалған құрылғыларды келесі тәсілдердің бірімен таңдаңыз:

   - Егер сіз белгілі бір басқару тобының барлық қосалқы Серверлері үшін тапсырма жасағыңыз келсе, сол топты таңдап, ол үшін топтық тапсырма құруды бастаңыз.

   - Егер сіз белгілі бір қосалқы Басқару серверлері үшін тапсырма жасағыңыз келсе, сол Серверлерді таңдап, олар үшін тапсырма жасаңыз.

6. **Таратылған орнату пакеттері** бетінде қосалқы Басқару серверлеріне көшіру қажет орнату пакеттерін таңдаңыз.

7. Осы есептік жазба астында *Орнату пакетін тарату* тапсырмасын іске қосу үшін есептік жазбаны көрсетіңіз. Сіз өзіңіздің есептік жазбаңызды қолданып, **Әдепкі есептік жазба** параметрін қосулы күйде қалдыра аласыз. Сонымен қатар, тапсырма қажетті қатынасу құқықтары бар басқа есептік жазбада орындалуы керек екенін көрсетуге болады. Ол үшін **Есептік жазбаны көрсету** параметрін таңдап, сол есептік жазбаның есептік деректерін енгізіңіз.

8. **Тапсырманы жасауды аяқтау** бетінде, тапсырма сипаттары терезесін ашу үшін **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосып, әдепкі бойынша тапсырма параметрлерін өзгертуге болады. Сондай-ақ, тапсырма параметрлерін кейінірек, кез келген уақытта конфигурациялауға болады.

9. **Аяқтау** түймесін басыңыз.

   Орнату пакеттерін қосалқы Басқару серверлеріне тарату үшін жасалған тапсырма тапсырмалар тізімінде көрсетіледі.

10. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Тапсырманы орындағаннан кейін, таңдалған орнату пакеттері көрсетілген қосалқы Басқару серверлеріне көшіріледі.

Қашықтан орнату тапсырмасын пайдаланып бағдарламаларды орнату

Kaspersky Security Center қашықтан орнату тапсырмаларын пайдаланып құрылғыларға бағдарламаларды қашықтан орнатуға мүмкіндік береді. Тапсырмалар шебердің көмегімен жасалады және құрылғыларға тағайындалады. Құрылғыларға (ең көбі 1000 құрылғы) тапсырманы тезірек және оңай тағайындау үшін құрылғы шебері терезесінде өзіңізге ыңғайлы түрде көрсете аласыз:

- **Басқару серверімен анықталған желілік құрылғыларды таңдау**. Құрылғылар жинағына тапсырма тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**. Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған таңдауды құрайтын құрылғыларға тағайындалады. Алдын ала анықталған таңдауды немесе өз таңдауыңызды көрсете аласыз.

- **Басқару тобына тапсырманы белгілеу**. Бұл жағдайда, тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады.

Қолданбаны желілік агент орнатылмаған клиент құрылғысына орнату кезінде туындауы мүмкін мәселелерге жол бермеу үшін Kaspersky Security Center қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру процедурасында сипатталғандай әрекет ету керек.

Бағдарламаны қашықтан орнату

Бұл бөлімде басқару тобындағы құрылғыларға, белгілі бір IP мекенжайлары бар құрылғыларға немесе басқарылатын құрылғылар жиынтығына бағдарламаны қашықтан орнату туралы ақпарат бар.

Бағдарламаны таңдалған құрылғыларға орнату үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.

3. **Тапсырма түрі** өрісінде **Бағдарламаны қашықтан орнату** таңдаңыз.

4. Келесі нұсқалардың бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

     Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

   Бағдарламаны қашықтан орнату тапсырмасы көрсетілген құрылғылар үшін жасалды. **Басқару тобына тапсырманы белгілеу** параметрін таңдаған болсаңыз, тапсырма топтық болып саналады.

5. **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғылар таңдауын көрсетіңіз.

   Қолжетімді параметрлер алдыңғы қадамда таңдалған параметрлерге байланысты.

6. **Орнату пакеттері** қадамында келесі параметрлерді көрсетіңіз:

   - Орнатылуы қажет бағдарламаның орнату пакетін **Орнату пакетін таңдау** өрісінен таңдаңыз.

   - **Орнату пакетін мәжбүрлеп жүктеп алу** параметрлер блогында бағдарламаны орнату үшін қажетті файлдарды клиент құрылғыларына жеткізу тәсілін таңдаңыз.

     - **Желілік агенттің көмегімен**

       Егер бұл параметр қосылса, орнату пакеттерін клиент құрылғыларына жеткізуді клиент құрылғыларына орнатылған Желілік агент жүзеге асырады.

       Егер бұл параметр өшірулі болса, орнату пакеттері клиент құрылғысының операциялық жүйесі құралдарының көмегімен жеткізіледі.

       Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

       Әдепкі бойынша, параметр қосулы.

     - **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

       Егер бұл параметр қосылса, орнату пакеттері тарату нүктелері арқылы операциялық жүйенің көмегімен клиент құрылғыларына беріледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл нұсқаны таңдауға болады.

       Желілік агент көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

       Әдепкі бойынша, параметр виртуалды Басқару серверінде жасалған қашықтан орнату тапсырмалары үшін қосылған.

       > Құрылғыға тағайындалған барлық тарату нүктелері ақаулы болған кезде, құрылғы жаңартуларды (антивирустық дерекқорлар мен патчтарды) және орнату пакеттерін алмайды.

     - **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

       Бұл параметр қосылса, файлдар Басқару сервері көмегімен клиент құрылғыларының операциялық жүйесі арқылы клиент құрылғыларына жеткізіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

       Әдепкі бойынша, параметр қосулы.

   - Басқару сервері файлдарды бір уақытта жібере алатын клиент құрылғыларының рұқсат етілген ең көп санын **Бір уақытта орындалатын жүктеулердің ең көп саны** өрісінде көрсетіңіз.

   - Орнату бағдарламасын іске қосуға рұқсат етілген ең көп санын **Орнату әрекеттерінің максималды саны** өрісінде көрсетіңіз.

     Тапсырма параметрлерінде көрсетілген әрекеттер саны асып кетсе, Kaspersky Security Center енді құрылғыдағы орнату қолданбасын іске қоспайды. *Бағдарламаны қашықтан орнату* тапсырмасын қайта іске қосу үшін **Орнату әрекеттерінің максималды саны** параметрінің мәнін арттырыңыз және тапсырманы орындаңыз. Сондай-ақ, сіз *Бағдарламаны қашықтан орнату* тапсырмасының басқасын жасай аласыз.

- Деректерді бір Kaspersky қолданбасынан екіншісіне тасымалдап жатсаңыз және ағымдағы қолданбаңыз құпиясөзбен қорғалған болса, **Kaspersky ағымдағы қолданбасын жою үшін құпиясөз** өрісіне құпиясөзді енгізіңіз. Ағымдағы Kaspersky қолданбасы деректерді тасымалдау кезінде жойылатынын ескеріңіз.

  Kaspersky ағымдағы қолданбасын жою үшін құпиясөз өрісі, **Орнату пакетін мәжбүрлеп жүктеп алу** параметрлер тобында **Желілік агенттің көмегімен** параметрін таңдаған жағдайда ғана қолжетімді болады.

  Жою құпиясөзін тек Қолданбаларды қашықтан орнату тапсырмасының көмегімен Kaspersky Endpoint Security for Windows орнату кезінде Kaspersky Security for Windows Server деректерін Kaspersky Endpoint Security for Windows қолданбасына көшіру сценарийі үшін ғана қолдана аласыз. Басқа компоненттерді орнату кезінде деинсталляция құпиясөзін пайдалану салдарынан орнату қателері туындауы мүмкін.

  Деректерді тасымалдау сценарийін сәтті аяқтау үшін келесі алғышарттардың орындалғанына көз жеткізіңіз:

  - Сіз Windows жүйесіне арналған Kaspersky Security Center Желілік агенті 14.2 немесе одан жоғары нұсқасын пайдаланып жатырсыз.
  - Сіз қолданбаны Windows басқаруымен жұмыс істейтін құрылғыларға орнатып жатырсыз.

- Қосымша параметрді конфигурациялаңыз:

  - **Бұрын орнатылып қойған жағдайда, бағдарламаны қайта орнатпау**

    Егер бұл параметр қосылса, таңдалған бағдарлама клиент құрылғысында орнатылған болса, қайта орнатылмайды.

    Егер бұл параметр өшірулі болса, бағдарлама кез келген жағдайда орнатылады.

    Әдепкі бойынша, параметр қосулы.

  - **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру**

    Файлдарды клиент құрылғыларына жібермес бұрын, Kaspersky Security Center бағдарламасы орнату утилитасының параметрлері клиент құрылғысының операциялық жүйесіне қолданылатындығын тексереді. Егер параметрлер қолданылмаса, Kaspersky Security Center бағдарламасы файлдарды жібермейді және бағдарламаны орнатуға тырыспайды. Мысалы, әртүрлі операциялық жүйелері бар құрылғыларды қамтитын басқару тобының құрылғыларынан кейбір бағдарламаларды орнату үшін басқару тобына орнату тапсырмасын тағайындауға болады, содан кейін қажеттіден басқа операциялық жүйесі бар құрылғыларды өткізіп жіберу үшін осы параметрді қосуға болады.

    Желілік агентті тағайындалмаған құрылғыларға қашықтан орнату кезінде Kaspersky Security Center немесе тарату нүктесі құрылғының операциялық жүйесінің түрін **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру** параметріне қарамастан автоматты түрде анықтайды.

  - **Active Directory топтық саясаттарында бума орнатуды тағайындау**

    Егер бұл параметр қосылса, орнату пакеті Active Directory топтық саясаттары арқылы орнатылады.

    Егер Желілік агенттің орнату пакеті таңдалса, параметр қолжетімді.

    Әдепкі бойынша, параметр өшірулі.

- **Пайдаланушылардан іске қосылған бағдарламаларды жабуды сұрайды**

  Іске қосылған бағдарламалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

- Бағдарламаны орнатқыңыз келетін құрылғыларды таңдаңыз:

  - **Барлық құрылғыларда орнату**

    Бағдарлама тіпті басқа Басқару серверлері басқаратын құрылғыларға орнатылады.

    Әдепкі бойынша, осы нұсқа таңдалады. Желіде тек бір Басқару сервері болса, бұл параметрді өзгертудің қажеті жоқ.

  - **Тек осы Басқару сервері арқылы басқарылатын құрылғыларда орнату**

    Бағдарлама тек осы Басқару сервері басқаратын құрылғыларға орнатылады. Егер сіздің желіңізде бірнеше Басқару сервері орнатылған болса және олардың арасындағы қайшылықтардан аулақ болғыңыз келсе, осы параметрді таңдаңыз.

- Орнатудан кейін, құрылғыларды басқару тобына жылжыту керектігін көрсетіңіз:

  - **Құрылғыларды жылжытпау**

    Құрылғылар тиесілі болып саналатын топтарда қалады. Топтардың ешқайсысына жатпайтын құрылғылар таратылмаған болып қалады.

  - **Тағайындалмаған құрылғыларды таңдалған топқа жылжыту (тек бір топты таңдауға болады)**

    Құрылғылар сіз таңдаған басқару тобына жылжытылады.

  Әдепкі бойынша **Құрылғыларды жылжытпау** нұсқасының таңдалғанын ескеріңіз. Қауіпсіздік тұрғысынан, сіз құрылғыларды қолмен жылжытуды таңдай аласыз.

7. Шебердің осы қадамында бағдарламаларды орнату кезінде құрылғыны қайта жүктеу талап етілетін көрсетіңіз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Келесі уақыттан кейін қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

8. Қажет болса, кезең-кезеңімен **Құрылғыларға қатынасу үшін есептік жазбаларды таңдау** қадамында *Бағдарламаны қашықтан орнату* тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

   - **Есептік жазба қажет емес (Желілік агент орнатылды)**

     Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

     Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

- **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

  Егер сіз қашықтан орнату тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда бағдарламаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

  - **Жергілікті есептік жазба**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті есептік жазба** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

    Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

  - **SSH сертификаты**. Бағдарламаны Linux басқаратын клиенттік құрылғыға орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

    Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Назар аударыңыз, Kaspersky Security Center, PEM жабық кілттері пішімін қолдайды, бірақ ssh-keygen утилитасы әдепкі бойынша OPENSSH пішіміндегі SSH кілттерін генерациялайды. OPENSSH пішімін Kaspersky Security Center қолдайды. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз. Мысалы:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<пайдаланушының электрондық поштасы>"
    ```

9. Тапсырма жасау және шеберді абу үшін **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

   Жасап болған соң, тапсырма туралы мәліметтерді ашу параметрі қосулы болса, тапсырма параметрлері терезесі ашылады. Бұл терезеде тапсырма параметрлерін тексеруге, оларды өзгертуге немесе қажет болса, тапсырманы іске қосу кестесін конфигурациялауға болады.

10. Тапсырмалар тізімінде жасалған тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес тапсырманың іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындағаннан кейін, таңдалған бағдарлама көрсетілген құрылғылар жиынтығына орнатылады.

Active Directory топтық саясаты арқылы бағдарламаны орнату

Kaspersky Security Center бағдарламасы Active Directory топтық саясаттарының көмегімен басқарылатын құрылғыларға Kaspersky бағдарламаларын орнатуға мүмкіндік береді.

> Active Directory топтық саясаттарының көмегімен бағдарламаларды орнату тек Желілік агент кіретін орнату пакеттерінен ғана мүмкін болады.

Бағдарламаны Active Directory топтық саясаттары көмегімен орнату үшін:

1. Қорғаныста орналастыру шеберін іске қосыңыз. Содан кейін, шебердің нұсқауларын орындаңыз.

2. Қорғаныста орналастыру шеберінің **«Қашықтан орнату» тапсырмасы параметрлері** бетінде **Active Directory топтық саясаттарында бума орнатуды тағайындау** параметрін таңдаңыз.

3. Құрылғыларға қатынасу үшін есептік жазбаларды таңдау бетінде **Есептік жазба қажет (Желілік агент пайдаланылмайды)** параметрін таңдаңыз.

4. Kaspersky Security Center бағдарламасы орнатылған құрылғыға немесе Иеленушілер-топтық саясатты жасаушылар домендік тобына кіретін есептік жазбаға әкімші құқықтары бар есептік жазбаны қосыңыз.

5. Таңдалған есептік жазбаға рұқсаттар беріңіз:

   a. **Басқару тақтасы** → **Басқару** тармағына өтіңіз және **Топтық саясатты басқару** тармағын ашыңыз.

   b. Қажетті домені бар түйінді басыңыз.

   c. **Табыстау** бөлімін басыңыз.

   d. **Қатынасу құқықтары** ашылмалы тізімінде **GPO байланыстырылған нысандары** тармағын таңдаңыз.

   e. **Қосу** түймесін басыңыз.

   f. Ашылған **Пайдаланушыны, компьютерді немесе топты таңдау** терезесінде қажетті есептік жазбаны таңдаңыз.

   g. **Пайдаланушыны, компьютерді немесе топты таңдау** терезесін жабу үшін **OK** түймесін басыңыз.

   h. **Топтар және пайдаланушылар** тізімінде жаңа ғана қосылған есептік жазбаны таңдаңыз және **Қосымша** → **Қосымша** түймесін басыңыз.

   i. **Рұқсаттар жазбалары** тізімінде жаңа ғана қосылған есептік жазбаны екі рет басыңыз.

   j. Келесі рұқсаттар беріңіз:

      - **топ нысандарын жасау;**
      - **топ нысандарын жою;**
      - **топтық саясат контейнерінің нысандарын жасау;**
      - **топтық саясат контейнерінің нысандарын жою.**

   k. Өзгерістерді сақтау үшін **OK** түймесін басыңыз.

6. Шебердің нұсқауларын орындай отырып, басқа параметрлерді белгілеңіз.

7. Жасалған қашықтан орнату тапсырмасын қолмен іске қосыңыз немесе оның кесте бойынша іске қосылуын күтіңіз.

Нәтижесінде, келесі қашықтан орнату механизмі іске қосылады:

1. Тапсырманы іске қосқаннан кейін, жиынтықтағы клиент құрылғылары тиесілі болып табылатын әр доменде келесі нысандар жасалады:

   - **Kaspersky_AK{GUID}** атты топтық саясат нысаны (Group policy object, GPO).
   - Қауіпсіздік тобында тапсырма таратылатын клиент құрылғылары бар. Бұл қауіпсіздік тобында тапсырма таратылатын клиент құрылғылары бар. Қауіпсіздік тобының құрамы топтық саясат нысаны (GPO) аймағын анықтайды.

2. Kaspersky Security Center таңдалған Kaspersky қолданбаларын клиент құрылғыларына тікелей KLSHARE арқылы, яғни қолданбаның желілік ортақ қатынасы бар қалтасынан орнатады. Бұл ретте, Kaspersky Security Center орнату қалтасында орнатылып жатқан бағдарлама үшін msi кеңейтімі бар файлды қамтитын салынған қосалқы қалта жасалады.

3. Тапсырманың әрекет ету ауқымына жаңа құрылғылар қосылған кезде, олар келесі тапсырманы іске қосқаннан кейін қауіпсіздік тобына қосылады. Егер тапсырманың кестесінде **Өткізіп алынған тапсырмаларды іске қосу** жалаушасы таңдалған болса, құрылғылар қауіпсіздік тобына бірден қосылады.

4. Құрылғыларды тапсырманың әрекет ету аумағынан алып тастаған кезде, оларды қауіпсіздік тобынан жою келесі тапсырманы іске қосқан кезде орын алады.

5. Тапсырманы Active Directory-ден жойған кезде топтық саясат нысаны (GPO), топтық саясат нысанына (GPO) келтірілген сілтеме және тапсырмамен байланысты қауіпсіздік тобы жойылады.

Егер сіз Active Directory арқылы басқа орнату схемасын қолданғыңыз келсе, орнату параметрлерін қолмен конфигурациялай аласыз. Бұл, мысалы, келесі жағдайларда қажет болуы мүмкін:

- әкімшіде кейбір домендердің Active Directory қызметіне өзгерістер енгізу құқығының антивирустық қорғанысы болмаған жағдайда;
- егер бастапқы дистрибутивті бөлек желілік ресурста орналастыру қажет болса;
- топтық саясатты Active Directory қызметінің нақты бөлімшелеріне байланыстыру.

Active Directory арқылы басқа орнату схемасын пайдаланудың келесі нұсқалары бар:

- Егер тікелей Kaspersky Security Center ортақ қатынасы бар қалтасынан орнату қажет болса, Active Directory топтық саясатының сипаттарында қажетті бағдарламаның орнату пакетінің қалтасына салынған exec қалтасында орналасқан msi кеңейтімі бар файлды көрсету керек.
- Егер орнату пакетін басқа желілік ресурсқа орналастыру қажет болса, оған exec қалтасының барлық мазмұнын көшіріп алу керек, өйткені MSI кеңейтімі бар файлдан басқа, ол орнату пакетін жасау кезінде қалыптасқан конфигурация файлдарын да қамтиды. Лицензиялық кілтті бағдарламамен бірге орнату үшін кілт файлын осы қалтаға көшіріп алу керек.

Қосалқы Басқару серверлеріне бағдарламаларды орнату

Бағдарламаны қосалқы Басқару серверлеріне орнату үшін:

1. Өзіңізге қажетті қосалқы Басқару серверлерін басқаратын Басқару серверіне қосылыңыз.

2. Орнатылған бағдарламаға сәйкес орнату пакеті таңдалған қосалқы Басқару серверлерінің әрқайсысында екеніне көз жеткізіңіз. Егер сіз кез келген Серверден орнату пакетін таба алмасаңыз, оны таратыңыз. Бұл үшін **Орнату пакетін тарату** тапсырма түрі бар тапсырманы жасаңыз.

3. Қосалқы Басқару серверлеріне бағдарламаны қашықтан орнату тапсырмасын жасаңыз. **Қосалқы Басқару серверіне бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.

   Жаңа тапсырма жасау шебері жұмысының нәтижесінде таңдалған қосалқы Басқару серверлеріне таңдалған бағдарламаны қашықтан орнату тапсырмасы жасалады.

4. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан орнату тапсырмасын орындағаннан кейін, таңдалған бағдарлама қосалқы Басқару серверлеріне орнатылады.

Unix басқаруымен жұмыс істейтін құрылғыларда қашықтан орнату параметрлерін көрсету

Бағдарламаны Unix басқаруымен жұмыс істейтін құрылғыға қашықтан орнату тапсырмасы арқылы орнатқан кезде, сіз осы тапсырма үшін Unix-ке тән параметрлерді көрсете аласыз. Бұл параметрлер тапсырма жасалғаннан кейін, оның сипаттарында қолжетімді.

Қашықтан орнату тапсырмасы үшін Unix-ке тән параметрлерді көрсету үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. Unix-ке тән параметрлерді көрсеткіңіз келетін қашықтан орнату тапсырмасының атын басыңыз.

   Тапсырма сипаттары терезесі ашылады.

3. **Бағдарлама параметрлері** → **Unix жүйесіне тән параметрлер** бөліміне өтіңіз.
4. Келесі параметрлерді белгілеңіз:

   - **Түбірлік есептік жазба үшін құпиясөз орнатыңыз (тек SSH арқылы орналастыру үшін)**

     `sudo` пәрменін мақсатты құрылғыда құпиясөзді көрсетпей қолдануға болмаса, осы параметрді таңдаңыз, содан соң root есептік жазбасы үшін құпиясөзді көрсетіңіз. Kaspersky Security Center бағдарламасы құпиясөзді мақсатты құрылғыға шифрланған түрде жібереді, құпиясөзді шифрсыздайды, содан кейін орнату процедурасын құпиясөзі көрсетілген root есептік жазбасы атынан іске қосады.

     > Kaspersky Security Center бағдарламасы SSH қосылымын жасау үшін есептік жазбаны немесе көрсетілген құпиясөзді пайдаланбайды.

   - **Мақсатты құрылғыда Рұқсатты орындау арқылы уақытша қалтаға жолды көрсетіңіз (тек SSH арқылы орналастыру үшін)**

     Егер мақсатты құрылғыдағы /tmp қалтасының Орындау құқығы болмаса, осы параметрді таңдап, содан кейін Орындау құқықтары бар қалта жолын көрсетіңіз. Kaspersky Security Center аталған қалтаны SSH арқылы қатынасу үшін уақытша қалта ретінде пайдаланады. Бағдарлама орнату пакетін қалтаға орналастырады және орнату процедурасын бастайды.

5. **Сақтау** түймесін басыңыз.

Көрсетілген тапсырма параметрлері сақталған.

Kaspersky бағдарламаларын іске қосу және тоқтату

Басқарылатын құрылғыларда Kaspersky қолданбаларын іске қосу және тоқтату үшін *қолданбаны іске қосу немесе тоқтату* тапсырмасын пайдалануға болады.

Қолданбаны іске қосу немесе тоқтату тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Ашылатын **Бағдарлама** тізімінен тапсырма жасағыңыз келетін қолданбаны таңдаңыз.

   Осы қолданбаларды басқаруға арналған веб-плагиндерді бұрын қосқан болсаңыз, Kaspersky қолданбалары тізімде пайда болады.
4. **Тапсырма түрі** тізімінде **Бағдарламаны белсендіру** тапсырмасын таңдаңыз.
5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
6. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.
7. **Бағдарламалар** терезесінде келесі әрекеттерді орындаңыз:
   - Тапсырма жасағыңыз келетін қолданбалардың атауларының жанындағы құсбелгілерді қойыңыз.
   - **Бағдарламаны іске қосу** немесе **Бағдарламаны тоқтату** параметрін таңдаңыз.
8. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** қадамында **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
9. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.
10. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.
11. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіп, параметрлерді сақтаңыз.

Тапсырма жасалды және конфигурацияланды.

Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

Ұялы құрылғыларды басқару

Kaspersky Security Center арқылы ұялы құрылғылардың қорғанысын басқару Ұялы құрылғыларды басқару құрамдасы арқылы жүзеге асырылады. Егер сіз ұйым қызметкерлеріне тиесілі ұялы құрылғыларды басқаруды жоспарласаңыз, Ұялы құрылғыларды басқаруды қосыңыз және конфигурациялаңыз.

Ұялы құрылғыларды басқару, қызметкерлердің Android құрылғыларын басқаруға мүмкіндік береді. Қорғанысты, құрылғыларда орнатылған Kaspersky Endpoint Security for Android мобильді қолданбасы қамтамасыз етеді. Бұл мобильді қолданба ұялы құрылғыларды веб-қауіптерден, вирустардан және қауіп төндіретін басқа бағдарламалардан қорғайды. Kaspersky Security Center Web Console арқылы орталықтандырылған басқару үшін Kaspersky Security Center Web Console бағдарламасы орнатылған құрылғыға келесі басқару веб-плагиндерін орнату қажет:

- Kaspersky Security for Mobile плагині
- Kaspersky Endpoint Security for Android плагині

Қорғанысты орналастыру және ұялы құрылғыларды басқару туралы ақпаратты Kaspersky Security for Mobile анықтамасынан қараңыз.

Kaspersky Security Center Web Console серверінде Ұялы құрылғыларды басқару параметрлерін өзгерту

Ұялы құрылғыларды басқару параметрлерін өзгерту үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Қосымша порттар** бөлімін таңдаңыз.

3. Қажетті параметрлерді өзгертіңіз:

   - **Ұялы құрылғыларға арналған портты ашу**

     Бұл ауыстырып қосқыш қосылса, мобильдік құрылғылар порты басқару серверінде ашық болады.

     Ұялы құрылғыларға арналған портты пайдалану, Ұялы құрылғыларды басқару құрамдасы орнатылған жағдайда ғана мүмкін болады.

     Бұл ауыстырып қосқыш өшірілсе, басқару серверіндегі мобильдік құрылғыларға арналған порт пайдаланылмайды.

     Әдепкісінше бұл ауыстырып-қосқыш өшірулі болады.

   - **Ұялы құрылғыны синхрондау порты**

     Ұялы құрылғылар Басқару серверіне қосылатын порт нөмірі. Әдепкі бойынша 13292-порт орнатылған.

     Ондық жазба нысаны қолданылады.

   - **Ұялы құрылғыларды белсендіруге арналған порт**

     Kaspersky Endpoint Security for Android қолданбасын Kaspersky белсендіру серверлеріне қосу порттары.

Әдепкі бойынша 17100-порт орнатылған.

4. **Сақтау** түймесін басыңыз.

Ұялы құрылғылар Басқару серверіне қосыла алады.

Үшінші тарап қауіпсіздік бағдарламаларын алмастыру

Kaspersky қауіпсіздік бағдарламаларын Kaspersky Security Center құралдарымен орнату үшін, орнатылатын бағдарламамен үйлеспейтін үшінші тарап бағдарламалық жасақтамасын жою қажет болуы мүмкін. Kaspersky Security Center, үшінші тарап бағдарламаларын жоюдың бірнеше тәсілін ұсынады.

Үйлесімсіз бағдарламаларды орнату бағдарламасы арқылы жою

Бұл параметр тек Microsoft Management Console басқару консолі негізіндегі Басқару консолінде қолжетімді.

Үйлесімді емес бағдарламалар жою әдісін әртүрлі орнату түрлері қолдайды. Қауіпсіздік бағдарламасын орнатпас бұрын, егер қауіпсіздік бағдарламасының орнату пакетінің сипаттары терезесінде (**Үйлесімді емес бағдарламалар** бөлімі) **Үйлесімді емес бағдарламаларды автоматты түрде жою** параметрі таңдалса, онымен үйлеспейтін бағдарламалар автоматты түрде жойылады.

Бағдарламаны қашықтан орнатуды кезінде үйлесімсіз бағдарламаларды жою

Қауіпсіздік бағдарламасын қашықтан орнату кезінде **Үйлесімді емес бағдарламаларды автоматты түрде жою** параметрін қосуға болады. Microsoft Management Console (MMC) консолі негізіндегі Басқару консолінде, бұл параметр қашықтан орнату шеберінде қолжетімді. Kaspersky Security Center Web Console бағдарламасында, бұл параметрді қорғанысты орналастыру шеберінде табуға болады Егер бұл параметр қосулы болса, Kaspersky Security Center бағдарламасы басқарылатын құрылғыға қауіпсіздік бағдарламасын орнатпас бұрын, үйлесімсіз бағдарламаларды жояды.

Нұсқаулар:

- Басқару консолі: үйлесімді емес бағдарламаларды қашықтан орнату шебері арқылы жою.
- Kaspersky Security Center Web Console: Орнатудың алдында үйлесімді емес бағдарламаларды жою.

Үйлесімсіз бағдарламаларды бөлек тапсырма арқылы жою

Үйлесімсіз бағдарламаларды жою үшін **Бағдарламаны қашықтан жою** тапсырмасы қолданылады. Тапсырма қауіпсіздік бағдарламасын орнату тапсырмасынан бұрын, құрылғыларда іске қосылуы керек. Мысалы, орнату тапсырмасында **Басқа тапсырманы аяқтағанда** түрі кестесін таңдауға болады, мұндағы басқа тапсырма – **Бағдарламаны қашықтан жою** тапсырмасы болып табылады.

Бұл жою тәсілі, қауіпсіздік бағдарламасы инсталляторы үйлесімсіз бағдарламалардың ешқайсысын сәтті жоя алмаған жағдайда қолданылғаны жөн.

Басқару консоліне арналған нұсқаулар: Жаңа тапсырма қосу.

Желідегі құрылғыларды табу

Бұл бөлімде құрылғыларды іздеу және желі сауалнамасы сипатталған.

Kaspersky Security Center белгіленген критерийлер негізінде құрылғыларды іздеуге мүмкіндік береді. Іздеу нәтижелерін мәтіндік файлға сақтауға болады.

Іздеу функциясы келесі құрылғыларды табуға мүмкіндік береді:

- Kaspersky Security Center Басқару сервері және оның қосалқы Серверлері топтарындағы басқарылатын құрылғылары;
- Kaspersky Security Center Басқару сервері мен оның қосалқы Серверлері басқаратын тағайындалмаған құрылғылар.

Сценарий: Желілік құрылғыларды табу

Қауіпсіздік бағдарламаларын орнатпас бұрын құрылғыларды іздеу керек. Басқару сервері анықталған құрылғылар туралы ақпаратты алады және саясаттардың көмегімен құрылғыларды басқаруға мүмкіндік береді. Желіде қолжетімді құрылғылар тізімін жаңарту үшін тұрақты желі сауалнамалары қажет.

> Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

Желілік құрылғыларды анықтау келесі кезеңдерді қамтиды:

1. **Құрылғыларды табу**

   Бағдарламаны жылдам іске қосу шебері құрылғыларды бастапқы табуды орындайды және компьютерлер, планшеттер және ұялы телефондар сияқты желілік құрылғыларды табуға көмектеседі. Сіз құрылғыларды табуды қолмен де іске қоса аласыз.

2. **Сауалнамалар кестесін конфигурациялау**

   Сауалнаманың қандай түрін үнемі қолданғыңыз келетінін анықтаңыз. Қажетті түрлерді қосыңыз және сауалнама кестесін конфигурациялаңыз. Сондай-ақ, желіде сауалнама өткізу жиілігі бойынша ұсыныстарды қараңыз.

3. **Табылған құрылғыларды басқару топтарына қосу ережелерін орнату (қажет болса)**

   Желіде жаңа құрылғылар пайда болса, олар әдеттегі сауалнамалар кезінде табылып, **Тағайындалмаған құрылғылар** тобына автоматты түрде қосылады. Құрылғыларды **Басқарылатын құрылғылар** тобына таратылатын құрылғыны жылжыту ережелерін конфигурациялауға болады. Сондай-ақ, сақтау ережелерін конфигурациялауға болады.

   3-қадамды өткізіп жіберсеңіз, жаңадан табылған құрылғылар тізімі **Тағайындалмаған құрылғылар** тобында орналасқан. Сіз осы құрылғыларды **Басқарылатын құрылғылар** тобына қолмен жылжыта аласыз. Құрылғыларды **Басқарылатын құрылғылар** тобына қолмен жылжытқан болсаңыз, онда сіз құрылғылардың әрқайсысы туралы ақпаратты талдап, оны басқару тобына және қайсысына жылжыту керектігін шеше аласыз.

Нәтижелер

Сценарийдің аяқталуы арқасында:

- Kaspersky Security Center Басқару сервері желідегі құрылғыларды анықтайды және олар туралы ақпарат береді.
- Желінің болашақ сауалнамалары және оларды іске қосу кестесі конфигурацияланды.
- Жаңадан табылған құрылғылар конфигурацияланған ережелерге сәйкес орналастырылады. (Болмаса ережелер конфигурацияланбаса, құрылғылар **Тағайындалмаған құрылғылар** тобында қалады).

Құрылғыларды табу

Бұл бөлімде Kaspersky Security Center бағдарламасында қолжетімді құрылғыларды анықтау түрлері сипатталған, сонымен қатар олардың әрқайсысын пайдалану туралы ақпарат берілген.

Тұрақты желілік сауалнамалар кезінде Басқару сервері желінің құрылымы мен желідегі құрылғылар туралы ақпарат алады. Деректер Басқару сервері дерекқорына жазылады. Басқару сервері желі сауалнамаларының келесі түрлерін жүргізе алады:

- **Windows желісінің сауалнамасы**. Басқару сервері Windows желісінің сауалнамасының екі түрін жүргізе алады: жылдам және толық. Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады. Толық сауалнама әрбір клиент құрылғысынан операциялық жүйенің атауы, IP мекенжайы, DNS атауы және NetBIOS атауы сияқты қосымша мәліметтерді сұрайды. Жылдам және толық сауалнама әдепкі бойынша қосылған. Windows желісінің сауалнамасы кезінде құрылғыларды анықтау мүмкін болмауы ықтимал, мысалы, роутер немесе желі экраны UDP 137, UDP 138, TCP 139 порттарын жауып тастаса.
- **Домен контроллерінің сауалнамасы**. Басқару сервері немесе тарату нүктесі домен құрылымы және доменге енгізілген құрылғылардың DNS атаулары туралы ақпаратты алады. Сауалнаманың бұл түрі әдепкі бойынша қосылған. Барлық желілік құрылғылар домен мүшелері болса, домен контроллерлері сұрауын пайдалану ұсынылады. Кейбір желілік құрылғылар доменге қосылмаған болса, бұл құрылғыларды домен контроллерлерін сұрау арқылы табу мүмкін емес.

- **IP ауқымдарының сауалнамасы**. Басқару сервері ICMP пакеттері немесе NBNS протоколдары арқылы көрсетілген IP ауқымдарына сауалнама жүргізеді және IP ауқымдарына кіретін құрылғылар туралы толық ақпарат алады. Сауалнаманың бұл түрі әдепкі бойынша өшірілген. Егер сіз Windows желісінің сауалнамасын және/немесе Active Directory сауалнамасын қолдансаңыз, сауалнаманың бұл түрін пайдалану ұсынылмайды.

- **Zeroconf сауалнамасы**. Тарату нүктесі нөлдік конфигурациясы бар желіні қолдана отырып, IPv6 желісіне сауалнама өткізеді (бұдан әрі *Zeroconf* деп те аталады). Сауалнаманың бұл түрі әдепкі бойынша өшірілген. Тарату нүктесі Linux жүйесінде жұмыс істеп тұрса, Zeroconf сауалнамасын пайдалануға болады.

Егер сіз құрылғыларды жылжыту ережелерін конфигурациялап, қосқан болсаңыз, табылған жаңа құрылғылар автоматты түрде **Басқарылатын құрылғылар** тобына ауысады. Егер құрылғыларды жылжыту ережелері қосылмаған болса, табылған жаңа құрылғылар автоматты түрде **Тағайындалмаған құрылғылар** тобына ауысады.

Әр түрге арналған құрылғыны анықтау параметрлерін өзгертуге болады. Мысалы, сауалнама кестесін өзгерту немесе бүкіл домендер тобына немесе тек белгілі бір доменге сауалнама жүргізу қажет екенін көрсету керек болуы мүмкін.

Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

Windows желісінің сауалнамасы

Windows желісінің сауалнамасы туралы

Жылдам сауалнама кезінде Басқару сервері желінің барлық домендері мен жұмыс топтары құрылғыларының NetBIOS атаулары тізімі туралы ақпаратты ғана алады. Толық сауалнама барысында, әрбір клиент құрылғысынан келесі ақпарат сұралады:

- Операциялық жүйенің аты
- IP мекенжайы
- DNS атауы
- NetBIOS атауы

Жылдам сауалнама кезінде де, толық сауалнама кезінде де керегі:

- UDP 137/138, TCP 139, UDP 445, TCP 445 ашық порттары.
- Қосулы SMB протоколы.
- Microsoft Computer Browser қызметі қолданылуы тиіс, ал негізгі браузер рөлін атқаратын құрылғы Басқару серверінде қолжетімді болуы керек;

- Microsoft Computer Browser қызметі қолданылуы тиіс, ал негізгі браузер рөлін атқаратын құрылғы клиент құрылғысында қолжетімді болуы керек:
  - Желілік құрылғылардың саны 32-ден аспаса, кемінде бір құрылғының болуы.
  - Әрбір 32 желілік құрылғыға кемінде бір құрылғының болуы.

Желінің толық сауалнамасы, егер жылдам сауалнама кемінде бір рет іске қосылған болса ғана іске қосылуы тиіс.

Windows желісінің сауалнамасы параметрлерін көру және өзгерту

Windows желісінің сауалнамасы параметрлерін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **Windows домендері** бөліміне өтіңіз.
2. **Сипаттар** түймесін басыңыз.

   Windows домені сипаттары терезесі ашылады.
3. **Windows желілік сауалнамасын қосу** қосқышын пайдалана отырып, Windows желісінің сауалнамасын қосыңыз немесе өшіріңіз.
4. Сауалнама кестесін конфигурациялаңыз. Әдепкі бойынша, жылдам сауалнама 15 минут сайын іске қосылады, ал толық сауалнама – 60 минут сайын.

   Сауалнама кестесінің нұсқалары:
   - **N күн сайын**

     Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

     Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.
   - **N минут сайын**

     Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.
   - **Апта күндері бойынша**

     Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.
   - **Ай сайын, таңдалған апталардың көрсетілген күндері**

     Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.
   - **Өткізіп алынған тапсырмаларды іске қосу**

     Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

     Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

     Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

Әдепкі бойынша, параметр өшірулі.

5. Windows желісінің сауалнамасы параметрлерін сақтаңыз.

Параметрлер сақталған және барлық Windows домендері мен жұмыс топтарына қатысты қолданылған.

Сауалнаманы қолмен іске қосу

Тексеруді дереу іске қосу үшін,

Жылдам сауалнаманы бастау немесе **Толық сауалнаманы бастау** түймесін басыңыз.

Сауалнама аяқталған кезде, сіз домен атының жанында жалаушаны қойып, **Windows домендері** бетінде анықталған құрылғылар тізімін қарап, **Құрылғылар** түймесін баса аласыз.

IP ауқымдарының сауалнамасы

Бастапқыда Kaspersky Security Center бағдарламасы өзі орнатылған құрылғының желілік параметрлерінен сауалнама өткізу үшін IP ауқымдарын алады. Құрылғы мекенжайы 192.168.0.1, ал ішкі желі бүркеніші 255.255.255.0 болса, онда Kaspersky Security Center бағдарламасы автоматты түрде 192.168.0.0/24 желісін сауалнамаға арналған мекенжайлар тізіміне қосады. Kaspersky Security Center бағдарламасы 192.168.0.1 және 192.168.0.254 аралығындағы барлық мекенжайларда сауалнама өткізеді.

Microsoft Active Directory немесе Samba домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` мен `workgroup` параметрлерін көрсетіңіз. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

Kaspersky Security Center бағдарламасы DNS кері іздеу немесе NBNS протоколы бойынша IP мекенжайлары ауқымдарында сауалнама жүргізе алады:

- **DNS кері іздеу;**

  Kaspersky Security Center бағдарламасы атауды кері түрлендіруді: көрсетілген ауқымдағы әрбір IP мекенжайы үшін стандартты DNS сұраулары арқылы DNS атауын түрлендіруді орындауға тырысады. Осы операция сәтті аяқталса, сервер `ICMP ECHO REQUEST` (ping пәрменінің баламасы) сұрауын алынған атауға жібереді. Егер құрылғы жауап берсе, бұл құрылғы туралы ақпарат Kaspersky Security Center дерекқорына қосылады. Атауды кері түрлендіру, IP мекенжайлары болуы мүмкін, бірақ желілік принтерлер немесе роутерлер сияқты компьютерлер болып саналмайтын желілік құрылғыларды алып тастау үшін қажет.

  Бұл сауалнама тәсілі дұрыс конфигурацияланған жергілікті DNS қызметіне негізделеді. Оны пайдалану үшін DNS кері қарау аймағы конфигурациялануы керек. Active Directory пайдаланылатын желілерде мұндай аймаққа автоматты түрде қолдау көрсетіледі. Бірақ, мұндай желілерде IP ішкі желісінің сауалнамасы Active Directory сауалнамасынан алынатын ақпараттан басқа қосымша ақпарат бермейді. Сонымен қатар, шағын желі әкімшілері көбінесе DNS кері қарау аймақтарын конфигурацияламайды, өйткені бұл көптеген желілік қызметтердің жұмыс істеуі үшін керек емес. Осы себептерге байланысты, IP ішкі желісінің сауалнамасы әдепкі бойынша өшірілген.

- **NBNS протоколы.**

  Егер желідегі атауларды кері шешу қандай да бір себептермен мүмкін болмаса, онда Kaspersky Security Center бағдарламасы IP ауқымдарының сауалнамасы үшін NBNS протоколын пайдаланады. Егер IP мекенжайына сұрау салу NetBIOS атауын қайтарса, бұл құрылғы туралы ақпарат Kaspersky Security Center дерекқорына қосылады.

Желіде сауалнама өткізуді бастамас бұрын SMB протоколының қосылғанына көз жеткізіңіз. Әйтпесе, Kaspersky Security Center бағдарламасы сауалнама өткізілетін желідегі құрылғыларды анықтай алмайды. SMB протоколын қосу үшін операциялық жүйеге арналған нұсқауларды орындаңыз.

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту

IP ауқымдарының сауалнамасы параметрлерін көру және өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру → Табу → IP ауқымдары** бөліміне өтіңіз.

2. **Сипаттар** түймесін басыңыз.

   IP ауқымдарының сауалнамасы сипаттары терезесі ашылады.

3. **Сауалнамаға рұқсат ету** ауыстырып-қосқышын қолдану арқылы IP ауқымдарының сауалнамасын қосыңыз немесе өшіріңіз.

4. Сауалнама кестесін конфигурациялаңыз. Әдепкі бойынша, IP ауқымдарының сауалнамасы 420 минут (жеті сағат) сайын іске қосылады.

   Сауалнама аралығын көрсеткен кезде, оның мәні IP мекенжайының әрекет ету уақыты параметрінің мәнінен аспайтынына көз жеткізіңіз. IP мекенжайы IP мекенжайының әрекет ету уақыты ішінде сауалнама өткізу кезінде расталмаса, ол сауалнама нәтижелерінен автоматты түрде жойылады. Әдепкі бойынша, сұраулардың қызмет ету мерзімі 24 сағатты құрайды, өйткені DHCP (Dynamic Host Configuration Protocol – желілік түйіннің динамикалық конфигурациясы протоколы) арқылы тағайындалған динамикалық IP мекенжайлары 24 сағат сайын өзгереді.

   Сауалнама кестесінің нұсқалары:

   - **N күн сайын**

     Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

     Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

   - **N минут сайын**

     Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

   - **Апта күндері бойынша**

     Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

   - **Ай сайын, таңдалған апталардың көрсетілген күндері**

     Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр өшірулі.

5. **Сақтау** түймесін басыңыз.

Параметрлер сақталады және барлық IP ауқымдарына қатысты қолданылады.

Сауалнаманы қолмен іске қосу

Тексеруді дереу іске қосу үшін,

Сауалнаманы бастау түймесін басыңыз.

IP ауқымын қосу және өзгерту

Бастапқыда Kaspersky Security Center бағдарламасы өзі орнатылған құрылғының желілік параметрлерінен сауалнама өткізу үшін IP ауқымдарын алады. Құрылғы мекенжайы 192.168.0.1, ал ішкі желі бүркеніші 255.255.255.0 болса, онда Kaspersky Security Center бағдарламасы автоматты түрде 192.168.0.0/24 желісін сауалнамаға арналған мекенжайлар тізіміне қосады. Kaspersky Security Center бағдарламасы 192.168.0.1 және 192.168.0.254 аралығындағы барлық мекенжайларда сауалнама өткізеді. Сіз автоматты түрде анықталған IP ауқымдарын өзгерте аласыз немесе өзіндік IP ауқымдарын қоса аласыз.

Ауқымды IPv4 мекенжайлары үшін ғана жасай аласыз. Zeroconf сауалнамасын қоссаңыз, Kaspersky Security Center бағдарламасы бүкіл желіде сауалнама өткізетін болады.

Жаңа IP ауқымын қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **IP ауқымдары** бөліміне өтіңіз.
2. IP ауқымын қосу үшін **Қосу** түймесін басыңыз.
3. Ашылған терезеде келесі параметрлерді конфигурациялаңыз:

   - **IP ауқым атауы**

     IP ауқым атауы. Сіз IP ауқымын атауы бойынша көрсете аласыз, мысалы, 192.168.0.0/24.

   - **IP аралығы немесе мекенжайы және ішкі желі бүркеніші**

     Бастапқы және соңғы IP мекенжайларын немесе ішкі желі мекенжайын және ішкі желі бүркенішін көрсету арқылы IP ауқымын белгілеңіз. **Шолу** түймесін басып, қолданыстағы IP мекенжайы ауқымдарының бірін де таңдай аласыз.

- **IP мекенжайының қызмет мерзімі (сағат)**

  Осы параметрді белгілеу кезінде, ол сауалнама кестесінде белгіленген сауалнама аралығының мәнінен асатынына көз жеткізіңіз. IP мекенжайы IP мекенжайының әрекет ету уақыты ішінде сауалнама өткізу кезінде расталмаса, ол сауалнама нәтижелерінен автоматты түрде жойылады. Әдепкі бойынша, сұраулардың қызмет ету мерзімі 24 сағатты құрайды, өйткені DHCP (Dynamic Host Configuration Protocol – желілік түйіннің динамикалық конфигурациясы протоколы) арқылы тағайындалған динамикалық IP мекенжайлары 24 сағат сайын өзгереді.

4. Егер сіз ішкі желіде немесе сіз көрсеткен аралықта сауалнама өткізгіңіз келсе, **IP ауқымы бойынша сауалнама өткізуді қосу** тармағын таңдаңыз. Әйтпесе, сіз қосқан ішкі желі немесе аралықта сауалнама өткізілмейді.

5. **Сақтау** түймесін басыңыз.

IP ауқымы IP ауқымдарының тізіміне қосылды.

Сауалнаманы бастау түймесін пайдаланып, әр IP ауқымы үшін бөлек сауалнама жүргізе аласыз. Сауалнама аяқталғаннан кейін, **Құрылғылар** түймесін басып, анықталған құрылғылар тізімін қарап шыға аласыз. Әдепкі бойынша, сауалнама нәтижелерінің жарамдылық мерзімі 24 сағатты құрайды және IP мекенжайының әрекет ету уақытына тең келеді.

Қолданыстағы IP ауқымына ішкі желіні қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **IP ауқымдары** бөліміне өтіңіз.

2. Ішкі желіні қосқыңыз келетін IP ауқымының атауын басыңыз.

3. Пайда болған терезеде **Қосу** түймесін басыңыз.

4. Ішкі желіні оның мекенжайы мен бүркеніші арқылы немесе IP ауқымындағы бірінші және соңғы IP мекенжайларын белгілеу арқылы көрсетіңіз. Не болмаса, **Шолу** түймесін басып, қолданыстағы ішкі желіні қосыңыз.

5. **Сақтау** түймесін басыңыз.

   Ішкі желі IP ауқымына қосылған.

6. **Сақтау** түймесін басыңыз.

IP ауқымы параметрлері сақталған.

Ішкі желілердің қалаған санын қоса аласыз. Аталған IP ауқымдары бір-бірімен қиылыспауы керек, бірақ IP ауқымдары ішіндегі атаусыз ішкі желілерге бұл шектеу қолданылмайды. Әрбір IP ауқымы үшін сауалнаманы дербес түрде қосуға немесе өшіруге болады.

Zeroconf сауалнамасы

Сауалнаманың бұл түріне тек Linux операциялық жүйелері бар тарату нүктелері үшін қолдау көрсетіледі.

Тарату нүктесі IPv6 мекенжайы бар құрылғыларға ие желілерді сұрастыра алады. Бұл жағдайда, IP ауқымдары көрсетілмейді, ал тарату нүктесі нөлдік конфигурациясы бар желіні (бұдан әрі *Zeroconf* деп те аталады) қолдану арқылы бүкіл желіде сауалнама жүргізеді. Zeroconf пайдалануды бастау үшін тарату нүктесінде avahi-browse утилитасын орнату керек.

IPv6 желісінде сауалнаманы қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру → Табу → IP ауқымдары** бөліміне өтіңіз.
2. **Сипаттар** түймесін басыңыз.
3. Ашылған терезеде **IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану** түймесін басыңыз.

Осыдан кейін, тарату нүктесі сіздің желіңізге сауалнама жүргізе бастайды. Бұл жағдайда, көрсетілген IP ауқымдары еленбейді.

Домен контроллері сауалнамасы

Kaspersky Security Center жүйесі Microsoft Active Directory домен контроллерлері мен Samba домен контроллерлерінің сұрауына қолдау көрсетеді.

> Kaspersky Security Center жүйесі Samba домен контроллерлерін тек Linux операциялық жүйесі бар тарату нүктесін пайдаланып сұрауға мүмкіндік береді. Samba домен контроллерлері үшін Active Directory домен контроллерлері ретінде Samba 4 пайдаланылады.

Домен контроллерін сұрау кезінде Басқару сервер немесе тарату нүктесі домен құрылымы, пайдаланушы тіркелгілері, қауіпсіздік топтары және доменге кіретін құрылғылардың DNS атаулары туралы ақпаратты алады.

Барлық желілік құрылғылар домен мүшелері болса, домен контроллерлері сұрауын пайдалану ұсынылады. Кейбір желілік құрылғылар доменге қосылмаған болса, бұл құрылғыларды домен контроллерлерін сұрау арқылы табу мүмкін емес.

Алдын ала талаптар

Домен контроллеріне сұрау салмас бұрын желілік экран немесе прокси-сервер арқылы домен контроллеріне қосылуға рұқсат бергеніңізге көз жеткізіңіз. Сондай-ақ, домен контроллерінде келесі протоколдардың қосылғанын тексеріңіз:

- Lightweight Directory Access Protocol (LDAP).
- Simple Authentication and Security Layer (SASL).

  Бұл протокол домен контроллері қосылымы SASL аутентификациясы арқылы орнатылған кезде пайдаланылады. Басқару сервері және тарату нүктелері тек DIGEST-MD5 механизмін қолдайды.
- Ақпаратты қорғау протоколы (LDAPS) арқылы Lightweight Directory Access Protocol

  Бұл протокол домен контроллеріне шифрланған қосылым арқылы қосылуыңыз қажет болған жағдайда пайдаланылады.

Домен контроллері құрылғысында келесі порттардың қолжетімді екеніне көз жеткізіңіз:

- LDAP протоколы және Simple Authentication (SASL қоса алғанда) үшін 389
- LDAPS протоколы үшін 636

Microsoft Active Directory немесе Samba домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` мен `workgroup` параметрлерін көрсетуіңіз керек. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

Егер Microsoft Active Directory доменінде бірнеше домен контроллері болса, доменді сұрау кезінде белгілі бір контроллерді таңдауға қолдау көрсетілмейді. Байланыс бірінші анықталған домен контроллерімен орнатылады. Microsoft Active Directory доменімен дұрыс аутентификацияны қамтамасыз ету үшін сертификаттың Subject Alternative Name (SAN) өрісі осы доменге енгізілген домен контроллерлерінің барлық мекенжайларын, сондай-ақ Microsoft Active Directory доменінің NetBIOS атауын қамтуы керек.

Басқару сервер көмегімен домен контроллерлерін сұрау

Әкімшілік серверін тек Microsoft Active Directory домен контроллерін сұрау үшін пайдалануға болады.

Басқару сервер арқылы домен контроллерлерін сұрау үшін:

1. Қолданбаның негізгі терезесінде **Табу және орналастыру → Табу → Домен контроллерлері** бөліміне өтіңіз.
2. **Сауалнама параметрлері** түймесін басыңыз.

   Домен контроллері сауалнамасының параметрлері терезесі ашылады.
3. **Домен контроллері сауалнамасын қосу** параметрін таңдаңыз.
4. **Қосымша параметрлер** бөлімінде сауалнама аймағын көрсетіңіз:
   - **Ағымдағы домен сауалнамасын жүргізу**

     Kaspersky Security Center иелігіндегі доменді сұрау үшін осы параметрді таңдаңыз.
   - **Бүкіл домендер тобының сауалнамасын жүргізу**

     Kaspersky Security Center тиесілі домендердің тобын сұрау үшін осы параметрді таңдаңыз.
   - **Көрсетілген домендер сауалнамасын жүргізу**

     Көрсетілген мекенжай және пайдаланушы есептік жазбасы деректері бар доменді сұрау үшін осы параметрді таңдаңыз.
5. Қажет болса, сауалнама кестесін реттеңіз. Әдепкі бойынша, сауалнама кезеңі бір сағатты құрайды. Әрбір кейінгі сауалнама кезінде алынған деректер алдыңғы деректерді толығымен алмастырады.

Желіде сауалнама өткізу кестесінің келесі нұсқалары қолжетімді:

- **N күн сайын**

  Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

  Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

- **N минут сайын**

  Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

- **Апта күндері бойынша**

  Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр өшірулі.

Доменнің қауіпсіздік тобындағы пайдаланушы есептік жазбасын өзгертсеңіз, бұл өзгерістер домен контроллерлері сауалнамасынан соң бір сағаттан кейін Kaspersky Security Center жүйесінде көрсетіледі.

6. Өзгерістерді қолдану үшін **Сақтау** түймесін басыңыз.

7. Желіде сауалнама өткізуді бірден іске қосу қажет болса, **Сауалнаманы бастау** түймесін басыңыз.

Тарату нүктесі көмегімен домен контроллерлерін сұрау

Сондай-ақ Microsoft Active Directory домен контроллерін және Samba домен контроллерін тарату нүктесін пайдаланып сұрауға болады. Windows немесе Linux жүйесімен басқарылатын құрылғы тарату нүктесі ретінде әрекет ете алады.

Linux тарату нүктесі үшін Microsoft Active Directory домен контроллері мен Samba домен контроллеріне сауалнама жүргізуге қолдау көрсетіледі.
Windows тарату нүктесі үшін тек Microsoft Active Directory домен контроллеріне сауалнама жүргізуге ғана қолдау көрсетіледі.
Mac тарату нүктесімен сауалнама жүргізуге қолдау көрсетілмейді.

Тарату нүктесі көмегімен домен контроллерлерінің сауалнамасын конфигурациялау үшін:

1. Тарату нүктесінің сипаттарын ашыңыз.
2. **Домен контроллерінің сауалнамасы** бөлімін таңдаңыз.
3. **Домен контроллері сауалнамасын қосу** параметрін таңдаңыз.
4. Сауалнама жүргізгіңіз келетін домен контроллерлерін таңдаңыз.

   Linux операциялық жүйесі бар тарату нүктесін пайдалансаңыз, **Көрсетілген домендер сауалнамасын жүргізу** бөлімінде **Қосу** түймесін басып, домен контроллерлерінің мекенжайы мен пайдаланушының тіркелгі деректерін көрсетіңіз.

   Windows операциялық жүйесі бар тарату нүктесін пайдалансаңыз, келесі нұсқалардың бірін таңдауға болады:

   - **Ағымдағы домен сауалнамасын жүргізу**
   - **Бүкіл домендер тобының сауалнамасын жүргізу**
   - **Көрсетілген домендер сауалнамасын жүргізу**
5. Қажет болса, сауалнама кестесінің параметрлерін көрсету үшін **Сауалнама кестесін орнату** түймесін басыңыз.

   Сауалнама кестеге сәйкес жүргізіледі. Сауалнаманы қолмен іске қосуға болмайды.

Сауалнама аяқталғаннан кейін, домен құрылымы **Домен контроллерлері** бөлімінде көрсетіледі.

Егер сіз құрылғыларды жылжыту ережелерін конфигурациялап, қосқан болсаңыз, табылған жаңа құрылғылар автоматты түрде **Басқарылатын құрылғылар** тобына ауысады. Егер құрылғыларды жылжыту ережелері қосылмаған болса, табылған жаңа құрылғылар автоматты түрде **Тағайындалмаған құрылғылар** тобына ауысады.

Анықталған пайдаланушы есептік жазбаларын Kaspersky Security Center Web Console ішіндегі домен аутентификациясы үшін пайдалануға болады.

Домен контроллерін аутентификациялау және қосу

Доменді сұрау кезінде аутентификация және домен контроллеріне қосылу

Linux операциялық жүйесімен жұмыс істейтін тарату нүктесі домен контроллеріне сауалнама жүргізгенде, тарату нүктесі домен контроллерімен бастапқы қосылымды орнату үшін қосылым протоколын анықтайды. Бұл протокол домен контроллерінің болашақтағы барлық қосылымдары үшін пайдаланылады. Домен контроллеріне бірінші рет қосылғанда, желілік агенттің жалаушаларын (`KLNAG_LDAP_TLS_REQCERT` және `KLNAG_LDAP_SSL_CACERT`) пайдаланып, қосылым опцияларын өзгертуге болады. Осы мақалада сипатталғандай, klscflag пәрменін пайдаланып, Желілік агент жалаушаларын конфигурациялауға болады.

Домен контроллеріне бастапқы қосылу келесідей іске асады:

1. Linux операциялық жүйесімен жұмыс істейтін тарату нүктесі LDAPS арқылы домен контроллеріне қосылуға әрекет етеді.

Әдепкі бойынша сертификатты тексеру қажет болмайды. Сертификатты мәжбүрлі түрде тексеру үшін `KLNAG_LDAP_TLS_REQCERT` жалаушасын 1 мәніне орнатыңыз.

`KLNAG_LDAP_TLS_REQCERT` жалаушасының ықтимал мәндері:

- `0` – сертификат сұралады, бірақ ол берілмесе немесе сертификатты тексеру сәтсіз аяқталса, TLS қосылымы әлі де сәтті жасалған деп саналады (әдепкі мән).
- `1` – LDAP сервері сертификатын қатаң тексеру қажет.

Әдепкісінше `KLNAG_LDAP_SSL_CACERT` жалаушасы белгіленбесе, сертификаттар тізбегіне қол жеткізу үшін сертификаттау орталығының (CA) операциялық жүйеге тәуелді жолы қолданылады. Басқа жолды көрсету үшін `KLNAG_LDAP_SSL_CACERT` жалаушасын пайдаланыңыз.

2. LDAPS қосылымы сәтсіз болса, Linux операциялық жүйесі бар тарату нүктесі SASL (DIGEST-MD5) көмегімен шифрланбаған TCP қосылымы арқылы домен контроллеріне қосылуға әрекет жасайды.

Жалаушаларды конфигурациялау

Жалаушаларды конфигурациялау үшін klscflag утилитасын пайдалануға болады.

Linux операциялық жүйесі бар тарату нүктесінде пәрмен жолын іске қосыңыз және ағымдағы каталогты klscflag утилитасы бар каталогқа өзгертіңіз. Әдепкісінше Linux операциялық жүйесі бар тарату нүктесінде klscflag утилитасы /opt/kaspersky/ksc64/sbin қалтасында орналасқан.

Мысалы, келесі пәрмен сертификатты мәжбүрлі түрде тексереді:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Samba домен контроллерлерін конфигурациялау

Kaspersky Security Center тек Samba 4 жүйесінде жұмыс істейтін Linux домен контроллерлеріне қолдау көрсетеді.

Samba домен контроллері Microsoft Active Directory домен контроллері сияқты схема кеңейтімдеріне қолдау көрсетеді. Samba 4 схема кеңейтімін пайдаланып, Samba домен контроллерінің Microsoft Active Directory домен контроллерімен толық үйлесімділігін қосуға болады. Бұл қадам міндетті емес.

> Samba домен контроллерінің Microsoft Active Directory домен контроллерімен толық үйлесімділігін қосу ұсынылады. Бұл Kaspersky Security Center және Samba домен контроллері арасындағы дұрыс әрекеттестікті қамтамасыз етеді.

Samba домен контроллерінің Microsoft Active Directory домен контроллерімен толық үйлесімділігін қосу үшін:

1. RFC2307 схема кеңейтімін пайдалану үшін келесі пәрменді орындаңыз:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Samba домен контроллерінде схеманы жаңартуды қосыңыз. Ол үшін `/etc/samba/smb.conf` файлына келесі жолды қосыңыз:

   ```
   dsdb:schema update allowed = true
   ```

Схеманы жаңарту қатемен аяқталса, master схемасы ретінде қызмет ететін домен контроллерін толық қалпына келтіру керек.

Samba домен контроллері ішіндегі барлық Linux негізіндегі хост үшін `/etc/samba/smb.conf` файлындағы `netbios name` мен `workgroup` параметрлерін көрсетіңіз. Әйтпесе сауалнама нәтижелері қайталанатын хосттарды қамтуы мүмкін.

Тағайындалмаған құрылғылар үшін сақтау ережелерін конфигурациялау

Windows желісінде сауалнамалар аяқталғаннан кейін, анықталған құрылғылар Тағайындалмаған құрылғылар басқару тобының ішкі топтарына орналастырылады. Бұл басқару тобы келесі жол бойынша орналасқан: **Табу және орналастыру → Табу → Windows домендері**. **Windows домендері** қалтасы тектік топ болып саналады. Қалтада, сауалнама барысында анықталған жұмыс топтары мен домендерге сай келетін атауларға ие еншілес топтар бар. Тектік топта ұялы құрылғыларды басқару топтары да болуы мүмкін. Сіз тектік басқару тобы үшін және әрбір еншілес топ үшін тағайындалмаған құрылғыларды сақтау ережелерін конфигурациялай аласыз. Сақтау ережелері, құрылғыларды табу параметрлеріне байланысты емес және тіпті құрылғыларды табу мүмкіндігі өшірулі болса да жұмыс істейді.

Құрылғыны сақтау ережелері, бір немесе бірнеше дискілері толық дискілік шифрлау арқылы шифрланған құрылғыларға әсер етпейді. Мұндай құрылғылар автоматты түрде жойылмайды – оларды тек қолмен жоюға болады. Шифрланған қатты дискісі бар құрылғыны жою қажет болса, алдымен дискінің шифрын шешіп, содан кейін құрылғыны алып тастаңыз.

Тағайындалмаған құрылғыларды сақтау ережелерін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру → Табу → Windows домендері** бөліміне өтіңіз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Тектік топ параметрлерін конфигурациялау үшін **Сипаттар** түймесін басыңыз.

     Windows домені сипаттары терезесі ашылады.

   - Еншілес топтың параметрлерін конфигурациялау үшін оның атауына басыңыз.

     Еншілес топ сипаттары терезесі ашылады.

3. Келесі параметрлерді конфигурациялаңыз:

   - **Мына уақыттан көбірек белсенді емес болса, құрылғыны топтан жойыңыз (тәулік)**

     Егер бұл параметр қосулы болса, құрылғы басқару тобынан автоматты түрде жойылатын уақыт аралығын көрсетуге болады. Әдепкі бойынша бұл параметр еншілес топтарға таралады. Әдепкі бойынша белгіленген уақыт аралығы – 7 күн.

     Әдепкі бойынша, параметр қосулы.

   - **Тектік топтан иелену**

     Бұл параметр өшірулі болса, ағымдағы топтағы құрылғылар үшін сақтау кезеңі тектік топтан иеленеді және өзгертіле алмайды.

     Бұл параметр тек еншілес топтар үшін ғана қолжетімді.

     Әдепкі бойынша, параметр қосулы.

- **Еншілес топтарда мәжбүрлеп иелену**

  Параметрлер мәндері еншілес топтарға бөлінеді, бірақ еншілес топтардың сипаттарында бұл параметрлер өзгертулер үшін қолжетімді емес.

  Әдепкі бойынша, параметр өшірулі.

4. **Қабылдау** түймесін басыңыз.

Сіздің өзгертулеріңіз сақталды және қолданылды.

Жабдықты түгендеу

Жабдықты түгендеу үшін қолданылатын жабдықтар тізімі (**Операциялар** → **Қоймалар** → **Жабдық**) екі тәсілмен толтырылады: автоматты түрде және қолмен. Әрбір желі сауалнамасынан кейін барлық анықталған құрылғы тізімге автоматты түрде қосылады; дегенмен желіде сауалнама өткізгіңіз келмесе, құрылғыларды қолмен қосуға болады. Тізімге маршрутизаторлар, принтерлер немесе құрылғы жабдықтары сияқты басқа құрылғыларды қолмен қосуға болады.

Құрылғының сипаттарында құрылғылар туралы толық ақпаратты көруге және өңдеуге болады.

Жабдықтар тізімінде келесі құрылғы түрлері болуы мүмкін:

- компьютерлер;
- ұялы құрылғылар;
- желілік құрылғылар;
- виртуалды құрылғылар;
- компьютер компоненттері;
- компьютерлік периферия;
- қосылатын құрылғылар;
- VoIP телефондары;
- желілік қоймалар.

Әкімші анықталған құрылғыларға *Корпоративтік кластың аппараттық жасақтамасы* белгісін беруі мүмкін. Бұл белгіні құрылғының сипаттарында қолмен тағайындауға немесе оны автоматты түрде тағайындау критерийлерін белгілеуге болады. Бұл жағдайда, *Корпоративтік кластың аппараттық жасақтамасы* белгісі құрылғының түрі бойынша белгіленеді.

Kaspersky Security Center жабдықты шығынға жазуға мүмкіндік береді. Ол үшін құрылғы сипаттарында **Шығынға жазылды** опциясын таңдаңыз. Мұндай құрылғы жабдықтар тізімінде көрсетілмейді.

Әкімші **Жабдық** қалтасындағы бағдарламаланатын логикалық контроллерлер (БЛК) тізімімен жұмыс істей алады. БЛК тізімдерімен жұмыс істеу туралы толық ақпарат *Kaspersky Industrial Cyber Security for Nodes пайдаланушы нұсқаулығында* келтірілген.

Жаңа құрылғылар туралы ақпаратты қосу

Желідегі жаңа құрылғылар туралы ақпаратты қосу үшін:

1. Негізгі мәзірде **Операциялар** → **Қоймалар** → **Жабдық** бөліміне өтіңіз.
2. **Жаңа құрылғы** терезесін ашу үшін **Қосу** түймесін басыңыз.
3. **Жаңа құрылғы** терезесінде, **Құрылғы түрі** ашылмалы тізімінде қосқыңыз келетін құрылғы түрін таңдаңыз.
4. **ОК** түймесін басыңыз.

   Жалпы бөліміндегі құрылғы сипаттары терезесі ашылады.
5. **Жалпы** бөлімінде құрылғы туралы деректерді енгізу өрістерін толтырыңыз. **Жалпы** бөлімінде келесі параметрлер қолжетімді:

   - **Корпоративтік құрылғы**. Егер сіз құрылғыға *Корпоративтік* белгісін бергіңіз келсе, жалаушаны қойыңыз. Осы белгі бойынша құрылғыларды **Жабдық** қалтасынан іздеуге болады.
   - **Шығынға жазылды**. Егер сіз құрылғының **Жабдық** қалтасындағы құрылғылар тізімінде пайда болуын қаламасаңыз, жалаушаны қойыңыз.
6. **Қолдану** түймесін басыңыз.

Жаңа құрылғы **Жабдық** бетінің жұмыс аймағында көрсетіледі.

Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау

Кәсіпорын құрылғыларын анықтау критерийлерін конфигурациялау үшін:

1. Негізгі мәзірде **Операциялар** → **Қоймалар** → **Жабдық** бөліміне өтіңіз.
2. **Жабдық** бетінің жоғарғы жағында **Корпоративтік құрылғылар үшін ережені орнату** сілтемесін басыңыз.

   Корпоративтік құрылғылар үшін ережені орнату панелі шақырылады.
3. **Корпоративтік құрылғылар үшін ережені орнату** панелінде **Құрылғы үшін корпоративтік құрылғы атрибутын автоматты түрде орнату** опциясын қосыңыз. *Корпоративтік* атрибуты автоматты түрде тағайындалатын құрылғы түрлерін көрсетіңіз.

   Бұл параметр желі сауалнамасы арқылы қосылған құрылғыларға ғана әсер етеді. Қолмен қосылған құрылғылар үшін *Корпоративтік* параметрін қолмен орнатыңыз.
4. **ОК** түймесін басыңыз.

Корпоративтік құрылғыларды анықтау критерийлері конфигурацияланған.

Kaspersky бағдарламасы: лицензиялау және белсендіру

Бұл бөлімде Kaspersky Security Center бағдарламасының Kaspersky басқарылатын бағдарламаларының лицензиялық кілттерімен жұмыс істеу мүмкіндіктері сипатталған.

Kaspersky Security Center бағдарламасы Kaspersky бағдарламаларының лицензиялық кілттерін клиент құрылғыларына орталықтан таратуға, кілттердің қолданылуын бақылау және лицензиялардың жарамдылық мерзімін ұзартуға мүмкіндік береді.

Kaspersky Security Center көмегімен лицензиялық кілт қосылған кезде лицензиялық кілттің сипаттары Басқару серверінде сақталады. Осы ақпарат негізінде бағдарлама лицензиялық кілттерді пайдалану туралы есепті қалыптастырады және әкімшіге лицензиялардың жарамдылық мерзімінің аяқталғаны және лицензиялық кілттердің сипаттарында қойылған лицензиялық шектеулердің асып кеткені туралы хабарлайды. Басқару сервері параметрлері құрамындағы лицензиялық кілттерді пайдалану туралы хабарландыру параметрлерін конфигурациялауға болады.

Басқарылатын бағдарламаларды лицензиялау

Басқарылатын құрылғыларда орнатылған Kaspersky бағдарламалары, бағдарламалардың әрқайсысына кілт файлын немесе белсендіру кодын қолдану арқылы іске қосылуы керек. Кілт файлы немесе белсендіру коды келесі тәсілдермен таратылуы мүмкін:

- Автоматты түрде тарату
- Басқарылатын бағдарламаның орнату пакетін пайдалану
- Басқарылатын бағдарламаның *Лицензиялық кілтін қосу* тапсырмасы арқылы
- Басқарылатын бағдарламаны қолмен белсендіру

Жоғарыда аталған тәсілдердің кез келгенімен белсенді немесе сақтық лицензиялық кілтті қосуға болады. Kaspersky бағдарламасы қазіргі уақытта белсенді болып саналатын кілтті пайдаланады және белсенді кілттің әрекет ету мерзімі аяқталғаннан кейін қолданылатын резервттегі лицензиялық кілтті сақтайды. Лицензиялық кілті қосылып жатқан бағдарлама кілттің белсенді немесе резервтік екенін анықтайды. Кілтті анықтау лицензиялық кілтті қосу үшін қолданылатын тәсілге байланысты емес.

Автоматты түрде тарату

Егер сіз әртүрлі басқарылатын бағдарламаларды қолдансаңыз және белгілі бір кілт файлын немесе белсендіру кодын құрылғыларға тарату маңызды болса, белсендіру кодын немесе кілтті таратудың басқа тәсілдерін қолданыңыз.

Kaspersky Security Center қолда бар лицензиялық кілттерді құрылғыларға автоматты түрде таратуға мүмкіндік береді. Мысалы, Басқару сервері қоймасында үш лицензиялық кілт бар. Барлық лицензиялық кілттер үшін **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасы қойылған. Ұйымның құрылғыларында Kaspersky қауіпсіздік бағдарламасы, мысалы, Kaspersky Endpoint Security for Windows орнатылған. Лицензиялық кілтті таратуды қажет ететін жаңа құрылғы табылды. Бағдарлама бұл құрылғыға не сәйкес келетінін анықтайды, мысалы, қоймадан екі лицензиялық кілт, *Кілт_1* лицензиялық кілті және *Кілт_2* лицензиялық кілті. Құрылғыға жарамды лицензиялық кілттердің бірі қолданылады. Бұл жағдайда, осы екі лицензиялық кілттің қайсысы осы құрылғыға қолданылатынын болжау мүмкін емес, өйткені лицензиялық кілттерді автоматты түрде тарату әкімшінің араласуын қамтымайды.

Лицензиялық кілтті құрылғыларға таратқан кезде осы лицензиялық кілт үшін құрылғылар есептеледі. Лицензиялық кілт қолданылатын құрылғылардың саны лицензиялық шектен аспайтынына көз жеткізуіңіз керек. Егер құрылғылардың саны лицензиялық шектен асып кетсе, мұндай құрылғыларға *Критикалық* күйі беріледі.

Таратпас бұрын, кілт файлы немесе белсендіру коды Басқару сервері қоймасына қосылуы керек.

Нұсқаулар:

- Басқару консолі:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті автоматты түрде тарату

  Немесе
- Kaspersky Security Center Web Console:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті автоматты түрде тарату

Келесі жағдайларда автоматты түрде таратылатын лицензиялық кілт виртуалды Басқару серверінің қоймасында көрінбеуі мүмкін екенін ескеріңіз:

- Лицензиялық кілт бағдарлама үшін жарамсыз.
- Виртуалды Басқару серверінде басқарылатын құрылғылар жоқ.
- Лицензиялық кілт басқа виртуалды Басқару сервері басқаратын құрылғылар үшін әлдеқашан қолданыста және құрылғылар санының лицензиялық шегіне жетті.

Басқарылатын бағдарламаның орнату пакетіне кілт файлын немесе белсендіру кодын қосу.

Қауіпсіздік тұрғысынан, бұл параметрді пайдалану ұсынылмайды. Орнату пакетіне қосылған кілт файлы немесе белсендіру коды бұзылуы мүмкін.

Басқарылатын бағдарламаны орнату пакеті арқылы орнатқан жағдайда, белсендіру кодын немесе кілт файлын орнату пакетінде немесе сол бағдарламаның саясатында көрсетуге болады. Лицензиялық кілт, құрылғыны Басқару серверімен кезекті рет синхрондау кезінде басқарылатын құрылғыларға қолданылады.

Нұсқаулар:

- Басқару консолі:
  - Орнату пакетін жасау
  - Клиент құрылғыларына бағдарламаларды орнату

  Немесе

- Kaspersky Security Center Web Console: Лицензиялық кілтті орнату пакетіне қосу.

Лицензиялы бағдарламалардың лицензиялық кілтін қосу тапсырмасы арқылы тарату

Басқарылатын бағдарламаның *Лицензиялық кілтін қосу* тапсырмасын пайдаланған жағдайда, сіз құрылғыларға таратылатын лицензиялық кілтті таңдап, құрылғыларды өзіңізге ыңғайлы тәсілмен таңдай аласыз, мысалы, басқару тобын немесе құрылғылар таңдауын таңдау арқылы.

Таратпас бұрын, кілт файлы немесе белсендіру коды Басқару сервері қоймасына қосылуы керек.

Нұсқаулар:

- Басқару консолі:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті клиент құрылғыларына тарату

  Немесе

- Kaspersky Security Center Web Console:
  - Лицензиялық кілтті Басқару серверінің қоймасына қосу
  - Лицензиялық кілтті клиент құрылғыларына тарату

Құрылғыларға белсендіру кодын немесе кілт файлын қолмен қосу.

Орнатылған Kaspersky бағдарламасын жергілікті түрде қосу үшін бағдарлама құралдарын пайдалануға болады. Кеңейтілген ақпаратты орнатылған бағдарламаларға арналған құжаттамадан қараңыз.

Лицензиялық кілтті Басқару серверінің қоймасына қосу

Басқару сервері қоймасына лицензиялық кілтті қосу үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Kaspersky лицензиялары** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Қосқыңыз келетін нәрсені таңдаңыз:
   - **Кілт файлын қосу**

     Кілт файлын таңдаңыз түймесін басып, қосқыңыз келетін .key файлын таңдаңыз.
   - **Белсендіру кодын енгізу**

     Мәтін жолағында белсендіру кодын көрсетіңіз және **Жіберу** түймесін басыңыз.
4. **Жабу** түймесін басыңыз.

Басқару сервері қоймасына лицензиялық кілт немесе бірнеше лицензиялық кілт қосылады.

Басқару серверінің лицензиялық кілтін қосу

Басқару серверінің лицензиялық кілтін қосу үшін:

1. Басқару серверінің мәнмәтіндік мәзірінде **Сипаттар** тармағын таңдаңыз.
2. Ашылған басқару сервері сипаттары терезесінде **Лицензиялық кілттер** бөлімін таңдаңыз.
3. **Белсенді лицензия кілті** бөлімінде **Өзгерту** түймесін басыңыз.
4. Ашылған терезеде **Қосу** түймесін басу арқылы лицензиялық кілт қосыңыз.

   Add license key wizard іске қосылады.

Шебер жұмысын аяқтағаннан кейін, функциялардың тиісті лицензияға сәйкес басқару консолінде көрсетілетінін тексеруге болады.

Лицензиялық кілтті клиент құрылғыларына тарату

Kaspersky Security Center Web Console қолданбасы лицензиялық кілтті клиент құрылғыларына автоматты түрде немесе **Бағдарламаны белсендіру** тапсырмасы арқылы таратуға мүмкіндік береді. Құрылғылардың белгілі бір тобына кілттерді тарату үшін тапсырманы пайдалануға болады. Лицензиялық кілтті тапсырманың көмегімен тарату кезінде құрылғылар санына қойылатын лицензия шектеу ескеріледі. Лицензия шегіне жеткенде Лицензиялық кілтін таратуды автоматты түрде тоқтату үшін автоматты кілтті таратуды пайдаланыңыз.

Лицензия кілтін автоматты түрде таратуды қосқан болсаңыз, лицензия кілтін клиент құрылғыларына тарату үшін **Бағдарламаны белсендіру** тапсырмасын жасамаңыз. Әйтпесе, жиі синхрондауға байланысты Басқару серверіне түсетін жүктеме артады.

Таратпас бұрын лицензиялық кілтті Басқару серверінің қоймасына қосыңыз.

*Лицензиялық кілтті клиент құрылғыларына **Бағдарламаны белсендіру** тапсырмасы арқылы тарату үшін:*

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. **Бағдарлама** ашылмалы тізімінде лицензия кілтін қосқыңыз келетін бағдарламаны таңдаңыз.
4. **Тапсырма түрі** тізімінде **Бағдарламаны белсендіру** тапсырмасын таңдаңыз.
5. **Тапсырманың атауы** өрісіне жаңа тапсырманың атын енгізіңіз.
6. Тапсырма тағайындалатын құрылғыларды таңдаңыз.
7. **Лицензия кілтін таңдау** шеберінің қадамында лицензия кілтін қосу үшін **Кілт қосу** сілтемесіне өтіңіз.
8. Кілт қосу тақтасында келесі параметрлердің бірін пайдаланып, лицензиялық кілт қосыңыз:

   Бағдарламаны белсендіру тапсырмасын жасағанға дейін басқару серверінің қоймасына лицензиялық кілтті қоспасаңыз ғана, лицензиялық кілтті қосу қажет.

   - Белсендіру кодын енгізу үшін **Белсендіру кодын енгізу** параметрін таңдаңыз, содан кейін келесі әрекеттерді орындаңыз:

     a. Белсендіру кодын көрсетіңіз және **Жіберу** түймесін басыңыз.

     Лицензиялық кілт туралы ақпарат кілтті қосу тақтасында көрсетіледі.

     b. **Сақтау** түймесін басыңыз.

     Лицензия кілтін басқарылатын құрылғыларға автоматты түрде таратуды қаласаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосыңыз.

     Кілт қосу тақтасы жабық.

   - Кілт файлын қосу үшін **Кілт файлын қосу** параметрін таңдаңыз, содан кейін келесі әрекеттерді орындаңыз:

     a. **Кілт файлын таңдаңыз** түймесін басыңыз.

     b. Ашылған терезеде кілт файлын таңдап, **Ашу** түймесін басыңыз.

     Лицензиялық кілт туралы ақпарат лицензиялық кілтті қосу тақтасында көрсетіледі.

c. **Сақтау** түймесін басыңыз.

Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде таратуды қаласаңыз, **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** параметрін қосыңыз.

Кілт қосу тақтасы жабық.

9. Кілттер кестесінен лицензиялық кілтті таңдаңыз.

10. Шебердің **Лицензия туралы ақпарат** қадамында белсенді лицензия кілтін ауыстырғыңыз келсе, әдепкі **Резервтік лицензия кілті ретінде пайдалану** құсбелгі ұяшығын алып тастаңыз.

    Мысалы, бұл ұйымыңыз өзгергенде және құрылғыда басқа ұйымның кілті қажет болғанда немесе кілт қайта шығарылған болса және ағымдағы лицензияның мерзімі біткенге дейін жаңа лицензияның мерзімі бітетін болса қажет. Қателерге жол бермеу үшін **Резервтегі лицензия кілті ретінде пайдалану** жалаушасын алып тастаңыз.

    Kaspersky Security Center қолданбасына кілт қосу кезінде туындауы мүмкін мәселелер және оларды шешу жолдары туралы көбірек білгіңіз келсе, Kaspersky Security Center білім қорын қараңыз.

11. **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қоссаңыз, тапсырма параметрлерінің орнатылған әдепкі мәндерін өзгертуге болады.

    Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Орнатылған әдепкі параметрлер мәндерін кейінірек өзгертуге болады.

12. **Аяқтау** түймесін басыңыз.

    Шебер жұмысының нәтижесінде тапсырма жасалды. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосулы болса, тапсырма параметрлерінің терезесі автоматты түрде ашылады. Бұл терезеде тапсырманың жалпы параметрлерін көрсетуге және қажет болса, тапсырма жасаған кезде көрсетілген параметрлерді өзгертуге болады.

    Тапсырмалар тізіміндегі жасалған тапсырма атауын басу арқылы тапсырма сипаттарының терезесін ашуға да болады.

    Тапсырма жасалып, орнатылып, тапсырмалар тізімінде көрсетіледі.

13. Тапсырманы іске қосу үшін тапсырмалар тізімінен тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

    Сондай-ақ тапсырма сипаттары терезесіндегі **Кесте** қойындысында тапсырманы іске қосу кестесін жасауға да болады.

    Кесте бойынша іске қосу параметрлерінің толық сипаттамасын тапсырманың жалпы параметрлерінен қараңыз.

Тапсырманы аяқтағаннан кейін, лицензиялық кілт таңдалған құрылғыларға таратылады.

Лицензиялық кілтті автоматты түрде тарату

Kaspersky Security Center бағдарламасы Басқару серверіндегі кілттер қоймасында орналастырылған лицензиялық кілттерді басқарылатын құрылғыларға автоматты түрде таратуға мүмкіндік береді.

Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату үшін

1. Бағдарламаның негізгі терезесінде **Операциялар → Лицензиялау → Kaspersky лицензиялары** бөліміне өтіңіз.

2. Құрылғыларға автоматты түрде таратқыңыз келетін лицензиялық кілттің атауын түртіңіз.

3. Ашылған лицензиялық кілттің сипаттары терезесінде **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасын қойыңыз.

4. **Сақтау** түймесін басыңыз.

Лицензиялық кілт сай келетін құрылғыларға автоматты түрде таратылатын болады.

Лицензиялық кілтті тарату Желілік агенттің құралдарымен орындалады. Бұл арада, бағдарлама үшін резервттегі лицензиялық кілтті тарату тапсырмалары жасалмайды.

Лицензиялық кілтті автоматты түрде тарату кезінде құрылғылар санына қойылатын лицензиялық шектеу ескеріледі. Лицензиялық шектеу лицензиялық кілттің сипаттарында белгіленген. Егер лицензиялық шектеуге қол жеткізілсе, лицензиялық кілтті құрылғыларға тарату автоматты түрде тоқтатылады.

Келесі жағдайларда автоматты түрде таратылатын лицензиялық кілт виртуалды Басқару серверінің қоймасында көрінбеуі мүмкін екенін ескеріңіз:

- Лицензиялық кілт бағдарлама үшін жарамсыз.
- Виртуалды Басқару серверінде басқарылатын құрылғылар жоқ.
- Лицензиялық кілт басқа виртуалды Басқару сервері басқаратын құрылғылар үшін әлдеқашан қолданыста және құрылғылар санының лицензиялық шегіне жетті.

Виртуалды Басқару сервері лицензиялық кілттерді өзінің қоймасынан және Басқару сервері қоймасынан автоматты түрде таратады. Ұсынылады:

- Құрылғыларға қолданғыңыз келетін лицензия кілтін таңдау үшін *Лицензия кілтін қосу* тапсырмасын пайдаланыңыз.
- Виртуалды Басқару серверінің параметрлеріндегі **Осы виртуалды Басқару серверінен өзінің құрылғыларына лицензиялық кілттерді автоматты түрде орналастыруға рұқсат беру** параметрін өшірмеңіз. Әйтпесе, виртуалды Басқару сервері лицензиялық кілттерді құрылғыларға, соның ішінде Басқару сервері қоймасынан лицензиялық кілттерді таратпайды.

Лицензиялық кілт сипаттары терезесінде **Лицензиялық кілтті басқарылатын құрылғыларға автоматты түрде тарату** жалаушасын қойылған болса, лицензиялық кілт сіздің желіңізде дереу таратылатын болады. Бұл параметрді таңдамасаңыз, лицензия кілтін тарату тапсырмасын кейінірек пайдалануға болады.

Негізгі Басқару серверінде конфигурацияланған лицензия кілттерін автоматты түрде тарату виртуалды емес қосалқы Басқару серверлері басқаратын құрылғыларды қамтымайды.

Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу

Басқару сервері қоймасына қосылған лицензиялық кілттердің тізімін көру үшін:

Бағдарламаның негізгі терезесінде **Операциялар → Лицензиялау → Kaspersky лицензиялары** бөліміне өтіңіз.

Басқару сервері қоймасына қосылған кілт файлдары мен белсендіру кодтарының тізімі көрсетіледі.

Лицензиялық кілт туралы толық ақпаратты көру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Лицензиялау → Kaspersky лицензиялары** бөліміне өтіңіз.
2. Қажетті лицензиялық кілттің атын басыңыз.

Ашылған лицензиялық кілттің сипаттары терезесінде сіз келесіні көре аласыз:

- **Жалпы** қойыншасында – лицензиялық кілт туралы негізгі ақпарат.
- **Құрылғылар** қойыншасында – орнатылған Kaspersky бағдарламасын белсендіру үшін лицензиялық кілт қолданылған клиент құрылғыларының тізімі.

Таңдалған клиент құрылғысында қандай лицензиялық кілттердің жиі кездесетінін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар) → Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Қажетті құрылғының атауын басыңыз.
3. Ашылған құрылғы сипаттары терезесінде **Бағдарламалар** қойыншасын таңдаңыз.
4. Таратылған лицензиялық кілт туралы ақпаратты көргіңіз келетін бағдарламаның атауын басыңыз.
5. Ашылған бағдарлама сипаттары терезесінде **Жалпы** қойыншасына өтіп, **Лицензия** бөлімін ашыңыз.

Белсенді және сақтық лицензиялық кілттер туралы негізгі ақпарат көрсетіледі.

Виртуалды Басқару серверінің лицензиялық кілттерінің өзекті параметрлерін анықтау үшін Басқару сервері тәулігіне бір реттен сиретпей Kaspersky белсендіру серверлеріне сұрау жібереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады.

Лицензия кілтін қоймадан өшіру

Басқару серверінің қосымша мүмкіндігі үшін, мысалы, Осалдықтар мен патчтарды басқару немесе Мобильдік құрылғыларды басқару мүмкіндігі үшін белсенді лицензиялық кілтті жойған кезде, тиісті функционалдылық қолжетімді болмайды. Резервттегі лицензия кілті қосылған болса, ол алдыңғы белсенді лицензия кілті өшірілгеннен кейін автоматты түрде белсенді болады.

Басқарылатын құрылғыға орналастырылған белсенді лицензиялық кілт жойылған кезде, қолданба басқарылатын құрылғыда жұмысын жалғастырады.

Басқару сервері қоймасынан кілт файлын немесе белсендіру кодын жою үшін:

1. Басқару сервері сіз жойғыңыз келетін кілт файлын немесе белсендіру кодын пайдаланбайтынына көз жеткізіңіз. Басқару сервері осындай кілтті қолданса, оны жоя алмайсыз. Тексеруді орындау үшін:

   a. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

   b. **Жалпы** қойыншасында **Лицензиялық кілттер** бөлімін таңдаңыз.

   c. Егер ашылған бөлімде қажетті кілт файлы немесе белсендіру коды көрсетілсе, **Белсенді кілтті жою** түймесін басып, операцияны растаңыз. Содан кейін басқару сервері қашықтағы лицензиялық кілтті пайдаланбайды, бірақ кілт басқару сервері қоймасында қалады. Егер қажетті кілт файлы немесе белсендіру коды көрсетілмесе, Басқару сервері оны пайдаланбайды.

2. Бағдарламаның негізгі терезесінде **Операциялар** → **Лицензиялау** → **Kaspersky лицензиялары** бөліміне өтіңіз.

3. Қажетті кілт файлын немесе белсендіру кодын таңдап, **Жою** түймесін басыңыз.

Таңдалған кілт файлы немесе белсендіру коды қоймадан жойылады.

Жойылған лицензиялық кілтті қайта қосуға немесе жаңа лицензиялық кілтті қосуға болады.

Лицензиялық келісімге берілген келісімді кері қайтарып алу

Егер сіз кейбір клиент құрылғыларын қорғауды тоқтатуды шешсеңіз, Kaspersky кез келген басқарылатын бағдарламасы үшін Лицензиялық келісімді кері қайтарып ала аласыз. Лицензиялық келісімді қайтарып алмас бұрын таңдалған бағдарламаны жою керек.

Виртуалды Басқару серверінде қабылданған Лицензиялық келісімдерді виртуалды Басқару серверінде немесе негізгі Басқару серверінде қайтарып алуға болады. Негізгі Басқару серверінде қабылданған Лицензиялық келісімдерді тек негізгі Басқару серверінде қайтарып алуға болады.

Kaspersky басқарылатын бағдарламалары үшін Лицензиялық келісімді кері қайтарып алу үшін:

1. Басқару сервері сипаттары терезесін ашып, **Жалпы** қойындысында **Түпкі пайдаланушының лицензиялық келісімдері** бөлімін таңдаңыз.

   Орнату пакеттерін жасау, жаңартуларды орнату немесе Kaspersky Security for Mobile қолданбасын орналастыру кезінде қабылданған Лицензиялық келісімдердің тізімі көрсетіледі.

2. Тізімнен қайтарып алғыңыз келетін Лицензиялық келісімдерді таңдаңыз.

   Лицензиялық келісімдердің келесі сипаттарын көруге болады:

   - Лицензиялық келісімді қабылдау күні.
   - Лицензиялық келісімді қабылдаған пайдаланушы аты.

3. Келесі деректерді көрсететін сипаттар терезесін ашу үшін кез келген Лицензиялық келісімнің қабылданған күнін басыңыз:

   - Лицензиялық келісімді қабылдаған пайдаланушы аты.
   - Лицензиялық келісімді қабылдау күні.
   - Лицензиялық келісімнің бірегей идентификаторы (UID).
   - Лицензиялық келісімнің толық мәтіні.
   - Лицензиялық келісімге қатысты нысандардың тізімі (орнату пакеттері, жаңартулар, ұялы қолданбалар) және олардың тиісті атаулары мен түрлері.

4. Лицензиялық келісімнің сипаттары терезесінің төменгі жағында **Лицензиялық келісімді қайтару** түймесін басыңыз.

   Лицензиялық келісімді қайтарып алуға мүмкіндік бермейтін қандай да бір нысандар (орнату пакеттері және олардың тиісті тапсырмалары) болса, тиісті хабарландыру көрсетіледі. Сіз бұл нысандарды жоймайынша, қайтарып алуды жалғастыра алмайсыз.

   Ашылған терезеде алдымен осы Лицензиялық келісімге сәйкес келетін Kaspersky бағдарламасын жою қажет екендігі туралы хабар көрсетіледі.

5. Лицензияны қайтарып алуды растайтын түймесін басыңыз.

Лицензиялық келісім қайтарып алынды. Лицензиялық келісім енді **Түпкі пайдаланушының лицензиялық келісімдері** бөліміндегі Лицензиялық келісімдер тізімінде көрсетілмейді. Лицензиялық келісімнің сипаттары терезесі жабылады; бағдарлама енді орнатылмайды.

Kaspersky бағдарламалары лицензиясының әрекет ету мерзімін ұзарту

Сіз мерзімі біткен немесе жақын арада аяқталатын (30 күннен аз) Kaspersky бағдарламасының лицензиясының жарамдылық мерзімін ұзарта аласыз.

Жарамдылық мерзімі жақын арада аяқталатын немесе аяқталған лицензияның мерзімін ұзарту үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Бағдарламаның негізгі терезесінде **Операциялар → Лицензиялау → Kaspersky лицензиялары** бөліміне өтіңіз.

   - Бағдарламаның негізгі терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз және хабарландырудың жанындағы **Жарамдылық мерзімі өтіп кеткен лицензияларды қарау** сілтемесінен өтіңіз.

   Kaspersky лицензиялары терезесі ашылып, онда лицензияның жарамдылық мерзімін қарай аласыз және ұзарта аласыз.

2. Қажетті лицензияның жанындағы **Лицензияны жаңарту** сілтемесінен өтіңіз.

   Лицензияның жарамдылық мерзімін ұзарту сілтемесін басу арқылы сіз Kaspersky бағдарламасына келесі Kaspersky Security Center деректерін беруге келісесіз: сіз қолданатын нұсқа, локализация, бағдарламалық жасақтама лицензиясының идентификаторы (яғни сіз жаңартып жатқан лицензия идентификаторы), сондай-ақ сіз лицензияны серіктес компания арқылы сатып алдыңыз ба, жоқ па.

3. Лицензияның жарамдылық мерзімін ұзартудың ашылған терезесінде нұсқауларды орындаңыз.

   Лицензияның жарамдылық мерзімі ұзартылды.

Kaspersky Security Center Web Console бағдарламасында хабарландырулар лицензияның жарамдылық мерзімінің аяқталуы келесі кесте бойынша жақындаған кезде көрсетіледі:

- жарамдылық мерзімінің аяқталу күніне дейін 30 күн бұрын;
- жарамдылық мерзімінің аяқталу күніне дейін 7 күн бұрын;
- жарамдылық мерзімінің аяқталу күніне дейін 3 күн бұрын;
- жарамдылық мерзімінің аяқталу күніне дейін 24 сағат бұрын;
- лицензия мерзімі өтіп кеткен кезде.

Бизнес шешімдерін таңдау үшін Kaspersky Marketplace пайдалану

Marketplace – Kaspersky бизнес-шешімдерінің барлық спектрін көруге, өзіңізге қажет шешімдерді таңдауға және Kaspersky сайтында сатып алуға өтуге мүмкіндік беретін бас мәзір бөлімі. Сіз сүзгілерді ұйымыңызға және ақпараттық қауіпсіздік жүйеңіздің талаптарына сәйкес келетін шешімдерді ғана көру үшін пайдалана аласыз. Шешімді таңдаған кезде, Kaspersky Security Center бағдарламасы сізді Kaspersky веб-сайтындағы тиісті бетке қайта бағыттайды, осылайша сіз шешім туралы көбірек біле алатын боласыз. Әрбір веб-бет сатып алуға өтуге мүмкіндік береді немесе сатып алу процесі туралы нұсқауларды қамтиды.

Marketplace бөлімінде Kaspersky шешімдерін келесі критерийлер бойынша сүзуге болады:

- Сіз қорғағыңыз келетін құрылғылардың саны (соңғы нүктелер, серверлер және активтердің басқа түрлері):
  - 50–250
  - 250–1000
  - 1000-нан артық
- Сіздің ұйымыңыздың ақпараттық қауіпсіздік тобының тәжірибе деңгейі:
  - **Foundations**

    Бұл деңгей тек АТ командасы бар кәсіпорындарға тән. Қауіптердің ең көп саны автоматты түрде бұғатталады.
  - **Optimum**

    Бұл деңгей АТ командасында нақты АТ қауіпсіздік функциясы бар кәсіпорынға тән. Бұл деңгейде компаниялар қолданыстағы алдын алу тетіктерін айналып өту үшін тауарлық қауіптер мен қауіптерге қарсы тұруға мүмкіндік беретін шешімдерді қажет етеді.
  - **Expert**

    Бұл деңгей күрделі және таратылған АТ ортасы бар кәсіпорындарға тән. АТ қауіпсіздік тобы тәжірибелі мамандардан тұрады немесе компанияда SOC (Security Operations Center) тобы бар. Қажетті шешімдер компанияларға кешенді қауіптер мен мақсатты шабуылдарға қарсы тұруға мүмкіндік береді.
- Қорғағыңыз келетін актив түрлері:
  - **Соңғы нүктелер**: қызметкерлердің жұмыс станциялары, физикалық және виртуалды машиналар, кіріктірілетін жүйелер.
  - **Серверлер**: физикалық және виртуалды серверлер.
  - **Cloud**: жария, жеке немесе гибридті бұлтты орталар; бұлттық қызметтер.
  - **Желі**: жергілікті желі, АТ инфрақұрылымы.
  - **Қызмет**: Kaspersky ұсынатын қауіпсіздікпен байланысты қызметтер.

Kaspersky бизнес шешімін табу және сатып алу үшін:

1. Бағдарламаның негізгі терезесінде **Marketplace** бөліміне өтіңіз.

   Әдепкі бойынша, бөлімде Kaspersky барлық қолжетімді бизнес-шешімдері көрсетіледі.
2. Ұйымыңызға сәйкес келетін шешімдерді ғана көру үшін сүзгілердегі қажетті мәндерді таңдаңыз.
3. Сатып алғыңыз келетін немесе көбірек білгіңіз келетін шешімді басыңыз.

Сіз шешімнің веб-бетіне қайта бағытталасыз. Сатып алуға өту үшін экрандағы нұсқауларды орындаңыз.

Желі қорғанысын конфигурациялау

Бұл бөлімде саясат пен тапсырмаларды қолмен конфигурациялау туралы, пайдаланушы рөлдері туралы, басқару топтарының құрылымын құру туралы және тапсырмалар иерархиясы туралы ақпарат бар.

Сценарий: Желі қорғанысын конфигурациялау

Бағдарламаны жылдам іске қосу шебері әдепкі бойынша параметрлері бар саясаттар мен тапсырмаларды жасайды. Бұл параметрлер ұйымда оңтайлы емес немесе тіпті тыйым салынған болуы мүмкін. Сондықтан, осы саясаттар мен тапсырмаларды конфигурациялау және сіздің желіңіз үшін қажет болса, қосымша саясаттар мен тапсырмаларды жасау ұсынылады.

Алдын ала талаптар

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

- Kaspersky Security Center Басқару серверін орнаттыңыз
- Kaspersky Security Center Web Console орнаттыңыз (қажет болса)
- Kaspersky Security Center орнатудың негізгі сценарийін орындадыңыз
- Бағдарламаны жылдам іске қосу шебері аяқталды немесе келесі саясаттар мен тапсырмалар **Басқарылатын құрылғылар** басқару тобында қолмен жасалған:
  - Kaspersky Endpoint Security саясаты
  - Kaspersky Endpoint Security жаңарту топтық тапсырмасы
  - Желілік агент саясаты
  - *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы

Желі қорғанысын конфигурациялау келесі кезеңдерден тұрады:

1. **Kaspersky бағдарламалары үшін саясаттар мен саясат профильдерін конфигурациялау және тарату**

   Басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялау және тарату үшін қауіпсіздікті басқарудың екі түрлі тәсілдемесін қолдануға болады: пайдаланушыға бағытталған және құрылғыға бағытталған. Осы екі тәсілдемені біріктіруге болады. Microsoft Management Console (MMC) басқару консолі және Kaspersky Security Center Web Console негізіндегі Басқару консолі құралдары құрылғыға бағытталған қауіпсіздікті басқару әдісін іске асыруға жарамды. Пайдаланушыға бағытталған қауіпсіздікті басқарудың әдісін іске асыру үшін тек Kaspersky Security Center Web Console жарамды.

2. **Kaspersky бағдарламаларын қашықтан басқару үшін тапсырмаларды конфигурациялау**

   Бағдарламаны жылдам іске қосу шеберімен жасалған тапсырмаларды тексеріп, қажет болған жағдайда олардың параметрлерін оңтайландырыңыз.

Нұсқаулар:

- Басқару консолі:
  - Kaspersky Endpoint Security жаңарту топтық тапсырмасын конфигурациялау
  - Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау
- Kaspersky Security Center Web Console:
  - Kaspersky Endpoint Security жаңарту топтық тапсырмасын конфигурациялау
  - Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері

Қажет болса, клиент құрылғыларында орнатылған Kaspersky бағдарламаларын басқарудың қосымша тапсырмаларын жасаңыз.

3. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын қолданбалар жұмысы кезінде пайда болатын оқиғалар туралы ақпарат клиент құрылғысынан тасымалданады және басқару серверінің дерекқорына тіркеледі. Басқару серверіне түсетін жүктемені азайту үшін дерекқорда сақталуы мүмкін оқиғалардың ең көп санын бағалаңыз және шектеңіз.

   Нұсқаулар:

   - Басқару консолі: Оқиғалардың ең көп санын конфигурациялау
   - Kaspersky Security Center Web Console: Оқиғалардың ең көп санын конфигурациялау

Нәтижелер

Осы сценарий аяқталғаннан кейін, сіздің желіңіз Kaspersky бағдарламаларын, Басқару сервері алатын тапсырмалар мен оқиғаларды конфигурациялау арқылы қорғалады:

- Kaspersky бағдарламалары саясаттар мен саясат профильдеріне сай конфигурацияланған.
- Бағдарламаларды басқару тапсырмалар жиынтығының көмегімен жүзеге асырылады.
- Дерекқорда сақталуы мүмкін оқиғалардың ең көп саны белгіленген.

Желі қорғанысын конфигурациялап болғаннан кейін, сіз Kaspersky дерекқорлары мен қолданбаларына арналған тұрақты жаңартуларды конфигурациялауға өте аласыз.

Kaspersky Sandbox-та анықталған қауіптерге автоматты түрде жауап беруді конфигурациялау туралы толық ақпаратты Kaspersky Sandbox 2.0 онлайн анықтамасынан қараңыз.

Құрылғыларға және пайдаланушыларға бағытталған қауіпсіздікті басқару тәсілдемелері

Қауіпсіздік параметрлерін құрылғының функциялары мен пайдаланушы рөлдері жайғасымынан басқаруға болады. Бірінші тәсілдемесі *құрылғыларға бағытталған қауіпсіздікті басқару*, екіншісі тәсілдемесі *пайдаланушыларға бағытталған қауіпсіздікті басқару* деп аталады. Бағдарламалардың әртүрлі параметрлерін әртүрлі құрылғыларға қолдану үшін, сіз тіркесімдегі бір немесе екі басқару түрін қолдана аласыз. Microsoft Management Console (MMC) басқару консолі және Kaspersky Security Center Web Console негізіндегі Басқару консолі құралдары құрылғыға бағытталған қауіпсіздікті басқару әдісін іске асыруға жарамды. Пайдаланушыға бағытталған қауіпсіздікті басқарудың әдісін іске асыру үшін тек Kaspersky Security Center Web Console жарамды.

Құрылғыға бағытталған қауіпсіздікті басқару құрылғының ерекшеліктеріне байланысты басқарылатын құрылғыларға қауіпсіздік бағдарламасының әртүрлі параметрлерін қолдануға мүмкіндік береді. Мысалы, әртүрлі басқару топтарында орналасқан құрылғыларға әртүрлі параметрлерді қолдануға болады. Сондай-ақ, құрылғыларды Active Directory-де немесе аппараттық жасақтаманың сипаттамалары бойынша пайдалану арқылы ажыратуға болады.

Пайдаланушыға бағытталған қауіпсіздікті басқару қауіпсіздік бағдарламаларының әртүрлі параметрлерін әртүрлі пайдаланушы рөлдеріне қолдануға мүмкіндік береді. Сіз бірнеше пайдаланушы рөлдерін жасай аласыз, әр пайдаланушыға сәйкес келетін пайдаланушы рөлін тағайындай аласыз және әртүрлі рөлдері бар пайдаланушыларға тиесілі құрылғылар үшін әртүрлі бағдарлама параметрлерін анықтай аласыз. Мысалы, бағдарламалардың әртүрлі параметрлерін бухгалтерлердің құрылғыларына және кадрлар бөлімі мамандарының құрылғыларына қатысты қолдануға болады. Пайдаланушыларға бағытталған қауіпсіздікті басқаруды енгізу нәтижесінде, әрбір бөлім – бухгалтерия бөлімі мен кадрлар бөлімі – Kaspersky бағдарламаларымен жұмыс істеуге арналған параметрлердің өзіндік конфигурациясын алады. Параметрлер конфигурациясы бағдарламаның қандай параметрлерін пайдаланушылар өзгерте алатынын, ал қайсысын әкімші мәжбүрлеп орнатып, бұғаттай алатынын анықтайды.

Пайдаланушыларға бағытталған қауіпсіздікті басқару жекелеген пайдаланушылар үшін белгіленген бағдарлама параметрлерін қолдануға мүмкіндік береді. Бұл, қызметкерге ұйымда бірегей рөл тағайындалса немесе белгілі бір қызметкерге қатысты қауіпсіздік мәселелерін бақылау керек болса, қажет болуы мүмкін. Бұл қызметкердің компаниядағы рөліне байланысты, бағдарламаның параметрлерін өзгерту үшін, оның құқықтарын кеңейтуге немесе қысқартуға болады. Мысалы, жергілікті кеңседе клиент құрылғыларын басқаратын жүйелік әкімшінің құқықтарын кеңейту қажет болуы мүмкін.

Сондай-ақ, сіз пайдаланушыларға бағытталған және құрылғыларға бағытталған қауіпсіздікті басқару тәсілдемелерін біріктіре аласыз. Мысалы, әрбір басқару тобы үшін әртүрлі саясаттарды конфигурациялауға, содан кейін ұйымыңыздың бір немесе бірнеше пайдаланушы рөлі үшін саясат профильдерін қосымша түрде жасауға болады. Бұл жағдайда, саясаттар мен саясат профильдері келесі тәртіпте қолданылады:

1. Құрылғыларға бағытталған қауіпсіздікті басқару үшін жасалған саясаттар қолданылады.

2. Олар саясат профильдерінің параметрлеріне сәйкес саясат профильдерімен түрлендіріледі.

3. Саясаттар пайдаланушы рөлдерімен байланысты саясат профильдерімен түрлендіріледі.

Саясаттарды конфигурациялау және тарату: құрылғыларға бағытталған тәсілдеме

Осы сценарий аяқталғаннан кейін, қолданбалар сіз анықтайтын қолданба саясаттары мен саясат профильдеріне сәйкес барлық басқарылатын құрылғыларда конфигурацияланады.

Алдын ала талаптар

Kaspersky Security Center Басқару серверін және Kaspersky Security Center Web Console веб-консолін (қажет болса) орнатқаныңызға көз жеткізіңіз. Kaspersky Security Center Web Console орнатқан болсаңыз, сізді құрылғыға бағытталған қауіпсіздікті басқаруға балама немесе қосымша ретінде пайдаланушыға бағдарланған қауіпсіздікті басқару да қызықтыруы мүмкін.

Кезеңдер

Құрылғыларға бағытталған Kaspersky бағдарламаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Бағдарламалар саясаттарын конфигурациялау**

   Әр бағдарлама үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялаңыз. Бұл саясат жиынтығы клиент құрылғыларына қолданылады.

   Бағдарламаны жылдам іске қосу шебері арқылы желі қорғанысын конфигурациялау кезінде Kaspersky Security Center бағдарламасы келесі бағдарламалар үшін әдепкі бойынша саясатты жасайды:

   - Kaspersky Endpoint Security for Windows – Windows операциялық жүйесі бар клиент құрылғылары үшін
   - Kaspersky Endpoint Security for Linux – Linux операциялық жүйесі бар клиент құрылғылары үшін

   Егер сіз осы шебердің көмегімен конфигурациялау процесін аяқтаған болсаңыз, сізге бұл бағдарлама үшін жаңа саясат жасаудың қажеті жоқ. Kaspersky Endpoint Security саясатын қолмен конфигурациялауға өтіңіз.

   Егер сізде бірнеше Басқару серверінің және/немесе басқару топтарының иерархиялық құрылымы болса, қосалқы Басқару серверлері мен еншілес басқару топтары саясатты әдепкі бойынша негізгі Басқару серверінен иеленеді. Саясат параметрлерін иерархия бойынша төмен қарай өзгертуге тыйым салу үшін параметрлерді еншілес топтар мен қосалқы Басқару серверлеріне мәжбүрлеп иелендіруге болады. Егер сіз параметрлердің тек бір бөлігін иеленуге рұқсат бергіңіз келсе, оларды саясат иерархиясы бойынша жоғары деңгейде құлыптай аласыз. Басқа құлыпталмаған параметрлер иерархия бойынша төменгі саясатты өзгерту үшін қолжетімді болады. Құрылған саясат иерархиясы басқару топтарындағы құрылғыларды тиімді басқаруға мүмкіндік береді.

   Нұсқаулар:

   - Басқару консолі: Саясат жасау
   - Kaspersky Security Center Web Console: саясат жасау

2. **Саясат профильдерін жасау (қажет болса)**

Егер сіз бір басқару тобындағы құрылғыларға әртүрлі саясат параметрлерін қолданғыңыз келсе, сол құрылғылар үшін саясат профильдерін жасаңыз. Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер басқарылатын құрылғыда әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды.

Профильді белсендіру шарттарын қолдана отырып, сіз әртүрлі саясат профильдерін қолдана аласыз, мысалы, белгілі бір бөлімшеде немесе Active Directory қауіпсіздік тобында орналасқан, белгілі бір бағдарламалық жасақтама конфигурациясы бар немесе белгіленген тегтері бар құрылғыларға. Белгілі бір өлшемшарттарға сәйкес келетін құрылғыларды сүзгілеу үшін тегтерді пайдаланыңыз. Мысалы, сіз *Windows* тегін жасай аласыз, оны Windows операциялық жүйесі басқаратын барлық құрылғыларға тағайындай аласыз, содан кейін бұл тегті саясат профилін белсендіру ережелерінде көрсете аласыз. Нәтижесінде, Windows операциялық жүйесі басқаратын құрылғыларда орнатылған Kaspersky бағдарламалары өздерінің саясат профилімен басқарылатын болады.

Нұсқаулар:

- Басқару консолі:
  - Саясат профилін жасау
  - Саясатын профилін белсендіру ережесін жасау
- Kaspersky Security Center Web Console:
  - Саясат профилін жасау
  - Саясатын профилін белсендіру ережесін жасау

3. **Саясаттар мен саясат профильдерін басқарылатын құрылғыларға тарату**

   Әдепкі бойынша, басқарылатын құрылғыларды Басқару серверімен синхрондау 15 минут сайын бір рет жүзеге асырылады. Автоматты синхрондауды өткізіп жіберіп, синхрондауды Мәжбүрлеп синхрондау пәрмені арқылы қолмен іске қосуға болады. Сондай-ақ, мәжбүрлеп синхрондау саясатты немесе саясат профилін жасағаннан немесе өзгерткеннен кейін орындалады. Синхрондау кезінде басқарылатын құрылғыларға жаңа немесе өзгертілген саясат пен саясат профильдері қолданылады.

   Kaspersky Security Center Web Console қолдансаңыз, саясат пен саясат профильдерінің құрылғыларға жеткізілгенін тексеруге болады. Kaspersky Security Center бағдарламасы құрылғының сипаттарында жеткізу күні мен уақытын анықтайды.

   Нұсқаулар:

   - Басқару консолі: Мәжбүрлеп синхрондау
   - Kaspersky Security Center Web Console: Мәжбүрлеп синхрондау

Нәтижелер

Құрылғыларға бағытталған сценарий аяқталғаннан кейін, Kaspersky бағдарламалары саясат иерархиясы арқылы көрсетілген және таралған параметрлерге сәйкес конфигурацияланады.

Бағдарлама саясаттары мен саясат профильдері басқару топтарына қосылған жаңа құрылғыларға автоматты түрде қолданылады.

Саясаттарды конфигурациялау және тарату: пайдаланушыларға бағытталған тәсілдеме

Бұл бөлімде басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларын орталықтандырылған конфигурациялауға арналған пайдаланушыға бағытталған сценарий сипатталған. Осы сценарий аяқталғаннан кейін, бағдарламалар сіз анықтайтын бағдарлама саясаттары мен саясат профильдеріне сәйкес барлық басқарылатын құрылғыларда конфигурацияланады.

Бұл сценарийді Kaspersky Security Center Web Console 13 және одан жоғары нұсқалары арқылы жүзеге асыруға болады.

Алдын ала талаптар

Kaspersky Security Center Басқару серверін және Kaspersky Security Center Web Console веб-консолін сәтті орнатқаныңызға және негізгі орнату сценарийін аяқтағаныңызға көз жеткізіңіз. Сондай-ақ, құрылғыға бағытталған қауіпсіздікті басқаруды пайдаланушыға бағытталған тәсілдемеге балама немесе қосымша мүмкіндік ретінде қарастырғыңыз келуі мүмкін. Басқарудың екі тәсілдемесі туралы көбірек біліңіз.

Процесс

Пайдаланушыға бағытталған Kaspersky бағдарламаларын басқару сценарийі келесі қадамдарды қамтиды:

1. **Бағдарламалар саясаттарын конфигурациялау**

   Әр бағдарлама үшін саясат жасау арқылы басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының параметрлерін конфигурациялаңыз. Бұл саясат жиынтығы клиент құрылғыларына қолданылады.

   Бағдарламаны жылдам іске қосу шебері арқылы желі қорғанысын конфигурациялау кезінде Kaspersky Security Center бағдарламасы Kaspersky Endpoint Security үшін әдепкі бойынша саясатты жасайды. Егер сіз осы шебердің көмегімен конфигурациялау процесін аяқтаған болсаңыз, сізге бұл бағдарлама үшін жаңа саясат жасаудың қажеті жоқ. Kaspersky Endpoint Security саясатын қолмен конфигурациялауға өтіңіз.

   Егер сізде бірнеше Басқару серверінің және/немесе басқару топтарының иерархиялық құрылымы болса, қосалқы Басқару серверлері мен еншілес басқару топтары саясатты әдепкі бойынша негізгі Басқару серверінен иеленеді. Саясат параметрлерін иерархия бойынша төмен қарай өзгертуге тыйым салу үшін параметрлерді еншілес топтар мен қосалқы Басқару серверлеріне мәжбүрлеп иелендіруге болады. Егер сіз параметрлердің тек бір бөлігін иеленуге рұқсат бергіңіз келсе, оларды саясат иерархиясы бойынша жоғары деңгейде құлыптай аласыз. Басқа құлыпталмаған параметрлер иерархия бойынша төменгі саясатты өзгерту үшін қолжетімді болады. Құрылған саясат иерархиясы басқару топтарындағы құрылғыларды тиімді басқаруға мүмкіндік береді.

   Нұсқаулар: саясатты жасау

2. **Пайдаланушыларды құрылғы иелері ретінде көрсетіңіз**

   Басқарылатын құрылғыларды сәйкес пайдаланушыларға тағайындаңыз.

   Нұсқаулар: Пайдаланушыны құрылғының иесі етіп тағайындау.

3. **Ұйымыңызға тән пайдаланушы рөлдерін анықтау**

   Ұйымыңыздың қызметкерлері әдетте орындайтын әртүрлі жұмыс түрлері туралы ойланыңыз. Сіз барлық қызметкерлерді олардың рөлдеріне сәйкес бөлуіңіз керек. Мысалы, сіз оларды бөлімдерге, кәсіптерге немесе лауазымдарға бөле аласыз. Осыдан кейін, сізге әр топ үшін пайдаланушы рөлін жасау қажет болады. Бұл жағдайда, әрбір пайдаланушы рөлінде осы рөлге тән бағдарлама параметрлерін қамтитын өзіндік саясат профилі болады.

4. **Пайдаланушы рөлдерін жасау**

   Алдыңғы қадамда сіз анықтаған әрбір қызметкерлер тобы үшін пайдаланушы рөлін жасаңыз және конфигурациялаңыз немесе алдын ала анықталған рөлдерді пайдаланыңыз. Пайдаланушы рөлдерінде бағдарлама мүмкіндіктеріне қатынасу құқықтарының жиынтығы бар.

   Нұсқаулар: Пайдаланушы рөлін жасау.

5. **Әрбір пайдаланушы рөлі үшін аймақты анықтау**

   Әрбір жасалған пайдаланушы рөлі үшін пайдаланушыларды және/немесе қауіпсіздік топтарын және басқару топтарын анықтаңыз. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

   Нұсқаулар: Пайдаланушы рөлі үшін аймақты өзгерту.

6. **Саясат профилін жасау**

   Ұйымыңыздың әрбір пайдаланушы рөлі үшін саясат профилін жасаңыз. Саясат профильдері әр пайдаланушының рөліне байланысты пайдаланушы құрылғыларында орнатылған бағдарламаларға қандай параметрлерді қолдану керектігін анықтайды.

   Нұсқаулар: Саясат профилін жасау.

7. **Саясат профилінің пайдаланушы рөлдерімен байланысы**

   Саясат профилінің профилін пайдаланушы рөлдерімен байланыстырыңыз. Осыдан кейін, саясат профилі осы рөл анықталған пайдаланушылар үшін белсенді болады. Саясат профилінің параметрлері пайдаланушының құрылғыларында орнатылған Kaspersky бағдарламаларына қолданылады.

   Нұсқаулар: Саясат профильдерінің рөлдермен байланысы.

8. **Саясаттар мен саясат профильдерін басқарылатын құрылғыларға тарату**

   Әдепкі бойынша, басқарылатын құрылғыларды Басқару серверімен синхрондау 15 минут сайын бір рет жүзеге асырылады. Синхрондау кезінде басқарылатын құрылғыларға жаңа немесе өзгертілген саясат пен саясат профильдері қолданылады. Автоматты синхрондауды өткізіп жіберіп, синхрондауды Мәжбүрлеп синхрондау пәрмені арқылы қолмен іске қосуға болады. Синхрондау аяқталғаннан кейін, саясаттар мен саясат профильдері жеткізіліп, Kaspersky белгіленген бағдарламаларына қолданылады.

   Саясаттар мен саясат профильдерінің құрылғыға жеткізілгенін тексеруге болады. Kaspersky Security Center бағдарламасы құрылғының сипаттарында жеткізу күні мен уақытын анықтайды.

   Нұсқаулар: Мәжбүрлеп синхрондау.

Нәтижелер

Пайдаланушыға бағытталған сценарий аяқталғаннан кейін, Kaspersky бағдарламалары саясаттар иерархиясы мен саясат профильдері арқылы көрсетілген және таралған параметрлерге сәйкес конфигурацияланады.

Жаңа пайдаланушы үшін, сізге есептік жазба жасау, пайдаланушыға жасалған пайдаланушы рөлдерінің бірін тағайындау және құрылғыларды пайдаланушыға тағайындау қажет. Бағдарлама саясаттары мен саясат профильдері сол пайдаланушының құрылғыларына автоматты түрде қолданылады.

Желілік агент саясатының параметрлері

Желілік агент саясаты параметрлерін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Желілік агент саясатының атауын басыңыз.

   Желілік агент саясатының сипаттары терезесі ашылады.

Пайдаланылатын операциялық жүйе түріне байланысты төмендегі параметрлердің қалай қолданылатынын егжей-тегжейлі сипаттайтын салыстыру кестесін қараңыз.

Жалпы

Бұл қойыншада саясаттың күйін өзгертуге және саясат параметрлерін иеленуді конфигурациялауға болады:

- **Саясаттың күйі** блогында саясаттың әрекет ету ауқымы нұсқаларының біреуін таңдауға болады:
  - **Белсенді**

    Осы нұсқа таңдалған болса, саясат белсенді болады.

    Әдепкі бойынша, осы нұсқа таңдалған.
  - **Белсенді емес**

    Егер бұл нұсқа таңдалса, саясат белсенді болмайды, бірақ **Саясат** қалтасында сақталады. Қажет болса, оны белсенді етуге болады.
- **Параметрлерді иелену** блогында саясатты иелену параметрлерін конфигурациялауға болады:
  - **Параметрлерді негізгі саясаттан иелену**

    Параметр қосулы болса, саясат параметрлері мәндері иерархияның жоғарғы деңгейіндегі топқа арналған саясаттан иеленеді және өзгерту үшін қолжетімді емес.

    Әдепкі бойынша, параметр қосулы.
  - **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену**

    Егер параметр қосылса, саясатқа өзгертулер қолданылғаннан кейін келесі қадамдар орындалады:
    - саясат параметрлерінің мәндері салынған басқару топтарының саясаты – еншілес саясаттарға қатысты қолданылады;
    - Әрбір еншілес саясат сипаттары терезесінің **Жалпы** бөлімінің **Параметрлерді иелену** блогында **Параметрлерді негізгі саясаттан иелену** параметрі автоматты түрде қосылады.

Параметр қосулы болған кезде, еншілес саясат параметрлерінің мәндерін өзгерту қолжетімді емес.

Әдепкі бойынша, параметр өшірулі.

Оқиғаларды конфигурациялау

Бұл қойыншада оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар **Оқиғаларды конфигурациялау** қойыншасындағы келесі бөлімдерде маңыздылық деңгейлері бойынша бөлінеді:

- **Функционалдық ақау**
- **Ескерту**
- **Ақпараттық**

Оқиғалар түрлері тізіміндегі әрбір бөлімде оқиғалардың атаулары және әдепкі бойынша Басқару серверінде оқиғаларды сақтау уақыты (күндерде) көрсетіледі. Оқиға түрін басқаннан кейін тізімде таңдалған оқиғаларды тіркеу және хабарландыру параметрлерін конфигурациялауға болады. Әдепкі бойынша, барлық Басқару сервері үшін көрсетілген жалпы хабарландыру конфигурациясы оқиғалардың барлық түрлері үшін қолданылады. Дегенмен, белгіленген оқиға түрлері үшін белгілі бір параметрлерді өзгертуге болады.

Мысалы, **Ескерту** бөлімінде **Қауіпсіздік мәселесі пайда болды** оқиға түрін конфигурациялауға болады. Мұндай оқиғалар, мысалы, тарату нүктесінің дискісіндегі бос орын 2 ГБ-тан аз болған кезде туындауы мүмкін (бағдарламаларды орнату және жаңартуларды қашықтан жүктеу үшін кемінде 4 ГБ қажет). **Қауіпсіздік мәселесі пайда болды** оқиғасын конфигурациялау үшін оған басып, орын алған оқиғаларды қайда сақтау керектігін және олар туралы қалай хабарлау керектігін көрсетіңіз.

> Желілік агент қауіпсіздік мәселесін анықтаса, сіз бұл қауіпсіздік мәселесін басқарылатын құрылғы параметрлері арқылы басқара аласыз.

Бағдарлама параметрлері

Параметрлер

Параметрлер бөлімінде Желілік агент саясатының параметрлерін конфигурациялауға болады:

- **Файлдарды тек тарату нүктелері арқылы тарату**

  Егер бұл параметр қосылса, басқарылатын құрылғылардағы Желілік агенттер жаңартуларды тек тарату нүктелерінен алады.

Егер бұл параметр өшірулі болса, басқарылатын құрылғылардағы Желілік агенттер тарату нүктелерінен немесе Басқару серверінен жаңартулар алады.

> Басқарылатын құрылғылардағы қауіпсіздік бағдарламалары әрбір қауіпсіздік бағдарламасы үшін жаңарту тапсырмасында белгіленген көзден жаңартуларды алатынын ескеріңіз. **Файлдарды тек тарату нүктелері арқылы тарату** параметрін қоссаңыз, Kaspersky Security Center бағдарламасы жаңарту тапсырмаларында жаңарту көзі ретінде орнатылғанына көз жеткізіңіз.

Әдепкі бойынша, параметр өшірулі.

- **Оқиғалар кезегінің максималды өлшемі, МБ**

  Өрісте оқиғалар кезегі болуы мүмкін дискідегі максималды орынды көрсетуге болады.

  Әдепкі бойынша, 2 МБ мәні көрсетілген.

- **Бағдарламаға құрылғыда саясаттың кеңейтілген деректерін шығарып алуға рұқсат берілген**

  Басқарылатын құрылғыға орнатылған Желілік агент, қолданылатын саясат туралы ақпаратты қауіпсіздік бағдарламасына жібереді (мысалы, Kaspersky Endpoint Security for Windows). Берілетін ақпарат қауіпсіздік бағдарламасының интерфейсінде көрсетіледі.

  Желілік агент келесі ақпаратты береді:

  - Саясатты басқарылатын құрылғыға жеткізу уақыты.
  - Саясатты басқарылатын құрылғыға жеткізу кезінде белсенді саясат атауы.
  - Басқарылатын құрылғыға саясатты жеткізу сәтіндегі кеңседен тыс саясаттың атауы (Linux жүйесіне арналған желілік агент үшін қолжетімді емес).
  - Саясатты басқарылатын құрылғыға жеткізу кезінде басқарылатын құрылғыға тиесілі басқару тобының атауы және толық жолы.
  - Басқарылатын құрылғыға саясатты жеткізу сәтіндегі атаулары мен басымдықтары бар белсенді саясат профильдерінің тізімі.

  Бұл ақпаратты, құрылғыға дұрыс саясатты қолдануды қамтамасыз ету үшін және ақауларды жою мақсатында пайдалана аласыз. Әдепкі бойынша, параметр өшірулі.

- **Желілік агент қызметін рұқсатсыз өшіруден немесе тоқтатудан қорғау және параметрлердегі өзгерістердің алдын алу**

  Желілік агент басқарылатын құрылғыға орнатылғаннан кейін, құрамдасты қажетті құқықтарсыз жою немесе өзгерту мүмкін емес. Желілік агенттің жұмысын тоқтату мүмкін емес. Бұл параметр домен контроллерлеріне әсер етпейді.

  Жергілікті әкімші құқықтарымен басқарылатын жұмыс станцияларында Желілік агентті қорғау үшін осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

- **Жою құпиясөзін пайдалану**

  Егер параметр қосулы болса, **Өзгерту** түймесін басқан кезде, желілік агентті қашықтан жою тапсырмасы үшін klmover утилитасына арналған құпия сөзді көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

Қоймалар

Қоймалар бөлімінде Желілік агент Басқару серверіне жіберетін нысандардың түрлерін таңдауға болады. Желілік агент саясатында, осы бөлімде көрсетілген параметрлерді өзгертуге тыйым салынса, бұл параметрлерді өзгерту мүмкін емес.

- **Орнатылған бағдарламалардың мәліметтері**

  Егер бұл параметр қосылса, клиент құрылғыларында орнатылған бағдарламалар туралы ақпарат Басқару серверге жіберіледі.

  Әдепкі бойынша, параметр қосулы.

- **Патчтар туралы ақпаратты қамту**

  Клиент құрылғыларында орнатылған бағдарлама патчтары туралы ақпарат Басқару серверіне жіберіледі. Бұл параметрді қосу, Басқару сервері мен ДҚБЖ-не түсетін жүктемені арттырып, дерекқор көлемінің ұлғаюына әкелуі мүмкін.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

- **Windows Update жаңартулар мәліметтері**

  Егер параметр орнатылған болса, Windows Update жаңартулары туралы ақпарат клиент құрылғыларына орнатылуы керек Басқару серверіне жіберіледі.

  Кейде параметр өшірулі болса да, жаңартулар **Қолжетімді жаңартулар** бөліміндегі құрылғы сипаттарында көрсетіледі. Бұл, мысалы, ұйымның құрылғыларында осы жаңартулар арқылы жабылуы мүмкін осалдықтар болса, орын алуы мүмкін.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер**

  Егер бұл параметр қосылса, басқарылатын құрылғыларда табылған үшінші тарап бағдарламаларындағы (Microsoft бағдарламалық жасақтамасын қоса) осалдықтар туралы ақпарат және осалдықтарды түзету бағдарламалық жасақтамасының жаңартулары (Microsoft бағдарламалық жасақтамасын қоспағанда) Басқару серверіне жіберіледі.

  Осы параметрді таңдау (**Бағдарламалық жасақтама осалдықтары мен сәйкес жаңартулар туралы мәліметтер**) желі жүктемесін, Басқару сервері дискісінің жүктемесін және Желілік агент ресурстарын тұтынуды арттырады.

  Әдепкі бойынша, параметр қосулы. Тек Windows үшін қолжетімді.

  Microsoft бағдарламаларының жаңартуларын басқару үшін **Windows Update жаңартулар мәліметтері** параметрін пайдаланыңыз

- **Жабдық тізімдемесі туралы ақпарат**

  Құрылғыға орнатылған Желілік агент құрылғының жабдықтары туралы ақпаратты Басқару серверіне жібереді. Жабдық туралы ақпаратты құрылғының сипаттарынан көруге болады.

  lshw утилитасы, жабдық туралы ақпарат алғыңыз келетін Linux құрылғыларында орнатылғанын тексеріңіз. Виртуалды машиналардан алынған жабдық туралы мәлімет пайдаланылатын гипервизорға байланысты толық болмауы мүмкін

Бағдарламалық жасақтаманың жаңартулары мен осалдықтары бөлімінде Windows жаңартуларын іздеуді және таратуды конфигурациялауға, сондай-ақ орындалатын файлдарда осалдықтардың бар-жоғын сканерлеуді қосуға болады:

- **Басқару серверін WSUS сервері ретінде пайдалану**

  Егер бұл параметр қосулы болса, Windows жаңартулары Басқару серверіне жүктеледі. Басқару сервері жүктелген жаңартуларды Желілік агенттер арқылы клиент құрылғыларындағы Windows Update қызметтеріне орталықтан ұсынады.

  Егер бұл параметр өшірулі болса, Басқару сервері Windows жаңартуларын жүктеу үшін пайдаланылмайды. Бұл жағдайда, клиент құрылғылары Windows жаңартуларын өздері алады.

  Әдепкі бойынша, параметр өшірулі.

- Windows Update жаңартулары көмегімен пайдаланушылар өз құрылғыларында қолмен орната алатын Windows Update жаңартуларын шектей аласыз.

  > Windows 10 операциялық жүйелері бар құрылғылар үшін, Windows Update-те құрылғыларға арналған жаңартулар табылса, онда сіз **Пайдаланушыларға Windows Update жаңартуларын орнатуды басқаруға рұқсат беру** астында таңдаған жаңа параметр, табылған жаңартуларды орнатқаннан кейін ғана қолданылады.

  Ашылмалы тізімнен параметрді таңдаңыз:

  - **Пайдаланушыларға барлық қолданылатын Windows Update жаңартуларын орнатуға рұқсат беру**

    Пайдаланушылар өз құрылғыларына қолданылатын барлық Windows Update жаңартуларын орната алады.

    Жаңартуларды орнатуға әсер еткіңіз келмесе, осы нұсқаны таңдаңыз.

    > Пайдаланушы Windows Update жаңартуларын қолмен орнатқан кезде, жаңартуларды Басқару серверінен емес, Microsoft серверлерінен жүктеуге болады. Бұл, Басқару сервері бұл жаңартуларды әлі жүктемеген болса жүзеге асырылуы мүмкін. Microsoft серверлерінен жаңартуларды жүктеу трафиктің өсуіне әкеледі.

  - **Пайдаланушыларға тек расталған Windows Update жаңартуларын орнатуға рұқсат беру**

    Пайдаланушылар өз құрылғыларына қолданылатын және әкімші мақұлдаған барлық Windows Update жаңартуларын орната алады.

    Мысалы, сіз алдымен жаңартуларды сынақ ортасында орнатуды тексеріп, олар құрылғылардың жұмысына кедергі келтірмейтіндігіне көз жеткізіп алып, содан кейін осы мақұлданған жаңартуларды клиент құрылғыларына орнатуға рұқсат бере аласыз.

    > Пайдаланушы Windows Update жаңартуларын қолмен орнатқан кезде, жаңартуларды Басқару серверінен емес, Microsoft серверлерінен жүктеуге болады. Бұл, Басқару сервері бұл жаңартуларды әлі жүктемеген болса жүзеге асырылуы мүмкін. Microsoft серверлерінен жаңартуларды жүктеу трафиктің өсуіне әкеледі.

- **Пайдаланушыларға Windows Update жаңартуларын орнатуға рұқсат бермеу**

  Пайдаланушылар Windows Update жаңартуларын өз құрылғыларына қолмен орната алмайды. Барлық қолданылатын жаңартулар әкімші белгілеген конфигурацияға сәйкес орнатылады.

  Жаңартуларды орнатуды орталықтан басқарғыңыз келсе, осы нұсқаны таңдаңыз.

  Мысалы, желіні жүктемеу үшін жаңарту кестесін конфигурациялауға болады. Пайдаланушылардың өнімділігіне кедергі келтірмеу үшін жаңартуларды жұмыс уақытынан тыс жоспарлауға болады.

- **Windows Update жаңартуларын іздеу режимі** параметрлер блогында жаңартуларды іздеу режимін таңдауға болады:

  - **Белсенді**

    Егер бұл нұсқа таңдалса, Басқару сервері Желілік агенттің көмегімен клиент құрылғысындағы Windows жаңарту агентінің жаңарту көзіне: Windows Update Servers немесе WSUS серверіне жүгінуін бастайды. Содан соң, Желілік агент Windows Update агентінен алынған ақпаратты Басқару серверіне жібереді.

    Бұл параметр, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы болса ғана қолданылады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **Пассив**

    Егер бұл нұсқа таңдалса, Желілік агент Windows жаңарту агентін жаңарту көзімен соңғы рет синхрондау кезінде алынған жаңартулар туралы ақпаратты мезгіл-мезгіл Басқару серверіне жібереді. Windows жаңарту агентін жаңарту көзімен синхрондау орындалмаса, Басқару серверіндегі жаңартулар туралы деректер ескіреді.

    Жаңарту көзі кэшінен жаңартуларды алғыңыз келсе, осы параметрді таңдаңыз.

  - **Өшірулі**

    Егер бұл нұсқа таңдалса, Басқару сервері жаңартулар туралы ақпаратты сұрамайды.

    Мысалы, алдымен жергілікті құрылғыдағы жаңартуларды тексергіңіз келсе, осы параметрді таңдаңыз.

- **Іске қосу кезінде орындалатын файлдарда осалдықтар бар-жоғын сканерлеу**

  Параметр қосулы болса, орындалатын файлдарды іске қосу кезінде олардың осалдығын тексеру жүргізіледі.

  Әдепкі бойынша, параметр қосулы.

Өшіріп қайта қосуды басқару

Қолданбаны дұрыс пайдалану, орнату не жою үшін басқарылатын құрылғының операциялық жүйесін өшіріп қосу қажет болса, **Өшіріп қайта қосуды басқару** бөлімінде орындалатын әрекетті көрсетуге болады.

- **Операциялық жүйені қайта жүктемеу**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Қажет болса, операциялық жүйені автоматты түрде қайта іске қосыңыз**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Осы уақыттан кейін мәжбүрлеп қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

    Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

    Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

    Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

    Әдепкі бойынша, параметр өшірулі.

Windows компьютерлік бөлісу қызметін пайдалану

Windows компьютерлік бөлісу қызметін пайдалану бөлімінде жұмыс үстелін бірлесіп пайдалану кезінде қашықтағы құрылғыда орындалатын әкімші әрекеттерінің аудитін қосуға және конфигурациялауға болады.

- **Аудитті қосу**

  Егер параметр қосулы болса, қашықтағы құрылғыдағы әкімші әрекетінің аудиті қосылады. Қашықтағы құрылғыдағы әкімші әрекеттері туралы жазбалар мында сақталады:

  - қашықтағы құрылғыдағы оқиғалар журналында;
  - қашықтағы құрылғыдағы Желілік агентті орнату қалтасында орналасқан syslog кеңейтімі бар файлда;
  - Kaspersky Security Center оқиғалар дерекқорында.

  Әкімші әрекеттерінің аудиті келесі шарттар орындалған кезде қолжетімді:

  - Осалдықтар мен патчтарды басқаруға арналған лицензия әлдеқашан қолданылады;
  - әкімшінің қашықтағы құрылғының жұмыс үстелін бірлесіп пайдалануға құқығы бар.

  Егер параметр өшірулі болса, қашықтағы құрылғыдағы әкімші әрекетінің аудиті өшіріледі.

  Әдепкі бойынша, параметр өшірулі.

- **Оқу кезінде бақыланатын файлдардың маскалары**

  Тізімде файл бүркеніштері сақталады. Аудит қосылған кезде, бағдарлама әкімшінің бүркеніштерге сәйкес келетін файлдарды оқуын қадағалайды және файлдарды оқу туралы ақпаратты сақтайды. **Аудитті қосу** жалаушасы қойылса, тізімді қолжетімді болады. Файл бүркеніштерін өзгертуге және тізімге жаңа бүркеніштер қосуға болады. Жаңа файл бүркеніштері тізімде жаңа жолдан көрсетілуі керек.

  Әдепкі бойынша *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf файлдарының бүркеніштері көрсетілген.

- **Өзгерткен кезде бақыланатын файлдардың маскалары**

  Тізімде қашықтағы құрылғыдағы файл бүркеніштері бар. Аудит қосылған кезде, бағдарлама әкімшінің бүркеніштерге сәйкес келетін файлдарды өзгертуін қадағалайды және файлдарды өзгерту туралы ақпаратты сақтайды. **Аудитті қосу** жалаушасы қойылса, тізімді қолжетімді болады. Файл бүркеніштерін өзгертуге және тізімге жаңа бүркеніштер қосуға болады. Жаңа файл бүркеніштері тізімде жаңа жолдан көрсетілуі керек.

  Әдепкі бойынша *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf файлдарының бүркеніштері көрсетілген.

Патчтарды және жаңартуларды басқару

Патчтарды және жаңартуларды басқару бөлімінде жаңартуларды алу мен таратуды және патчтарды басқарылатын құрылғыларға орнатуды конфигурациялауға болады:

- **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату**

  Егер жалауша қойылса, *Анықталмаған* мақұлдау мәртебесі бар Kaspersky патчтары жаңарту серверлерінен жүктелгеннен кейін автоматты түрде басқарылатын құрылғыларға орнатылады.

  Егер жалауша алынып тасталса, *Анықталмаған* мәртебесі бар Kaspersky жүктелген патчтары, әкімші олардың мәртебесін *Расталды* деп өзгерткеннен кейін орнатылады.

Әдепкі бойынша, параметр қосулы.

- **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)**

  Параметр қосулы болса, жаңартуларды алуға арналған офлайн-модель қолданылады. Басқару сервері жаңартуларды алған кезде, ол Желілік агентті (ол орнатылған құрылғыларда) басқарылатын бағдарламалар үшін қажет етілетін жаңартулар туралы хабардар етеді. Желілік агенттер жаңартулар туралы ақпаратты алған кезде, олар Басқару серверінен қажетті файлдарды ертерек жүктеп алады. Бірінші рет қосылған кезде, Сервер осы Агенттің жаңартуларды жүктеуіне түрткі болады. Желілік агент клиент құрылғысында барлық жаңартуларды жүктегеннен кейін, жаңартулар құрылғыдағы бағдарламалар үшін қолжетімді болады.

  Клиент құрылғысындағы басқарылатын бағдарлама жаңартуларды алу үшін Желілік агентке жүгінген кезде, Агент өзінде қажетті жаңартулардың бар ма екенін тексереді. Жаңартулар басқарылатын бағдарлама сұрау салған сәттен бастап 25 сағаттан ерте болмайтын мерзімнің ішінде Басқару серверінен алынған болса, онда Желілік агент Басқару серверіне қосылмайды және басқарылатын бағдарламаға жергілікті кэштегі жаңартуларды ұсынады. Желілік агент бағдарламаларға арналған жаңартуларды клиент құрылғыларында ұсынса, бірақ жаңарту үшін қосылым талап етілмесе, Басқару серверімен қосылым орындалмауы мүмкін.

  Параметр өшірулі болса, жаңартуларды жүктеп алудың офлайн үлгісі пайдаланылмайды. Жаңартулар, жаңартуларды жүктеу тапсырмасының кестесіне сәйкес таратылады.

  Әдепкі бойынша, параметр қосулы.

Қосылым мүмкіндігі

Қосылым мүмкіндігі бөлімі үш ішкі бөлімді қамтиды:

- **Желі**
- **Байланыс профильдері**
- **Байланыс кестесі**

Желі бөлімінде Басқару серверіне қосылым параметрлерін конфигурациялауға, UDP портын пайдалану мүмкіндігін қосуға және оның нөмірін көрсетуге болады.

- **Басқару серверіне қосылу** блогында Басқару серверіне қосылу параметрлерін конфигурациялауға және клиент құрылғыларының Басқару серверімен синхрондау кезеңін көрсетуге болады:

  - **Синхрондау аралығы (мин)**

    Желілік агент басқарылатын құрылғыларды Басқару серверімен синхрондайды. Синхрондау кезеңін (мерзімді сигнал) 10 000 басқарылатын құрылғыға 15 минутқа тең етіп белгілеу ұсынылады.

  - **Желілік трафикті қысу**

    Егер параметр өшірулі болса, Желілік агент деректерін беру жылдамдығы арттырылады, берілетін ақпарат көлемі азайтылады және Басқару серверіне түсетін жүктемені азайтады.

    > Клиент компьютерінің орталық процессорына түсетін жүктеме артуы мүмкін.

    Әдепкі бойынша, жалауша қойылған.

- **Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу**

  Параметр қосылса, Желілік агент пен Басқару серверінің жұмысына қажетті порттар Microsoft Windows брандмауэрінің ерекшеліктер тізіміне қосылады.

  Әдепкі бойынша, параметр қосулы.

- **SSL байланысын пайдалану**

  Бұл параметр қосулы болса, Басқару серверіне қосылу SSL протоколының көмегімен, қорғалған порт арқылы орындалатын болады.

  Әдепкі бойынша, параметр қосулы.

- **Әдепкі байланыс параметрлері астындағы тарату нүктесіндегі (қолжетімді болса) байланыс шлюзін пайдаланыңыз**

  Егер параметр қосулы болса, онда параметрлері басқару тобының сипаттарында белгіленген тарату нүктесінің қосылым шлюзі қолданылады.

  Әдепкі бойынша, параметр қосулы.

- **UDP портын пайдалану**

  Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

- **UDP портының нөмірі**

  Өрісте UDP портының нөмірін енгізуге болады. Әдепкі бойынша 15000-порт орнатылған.

  Ондық жазба нысаны қолданылады.

  Егер клиент құрылғысы Windows XP Service Pack 2 операциялық жүйесінің басқаруымен жұмыс істесе, кірістірілген желілік экран 15000 нөмірі бар UDP портын бұғаттайды. Бұл портты қолмен ашу керек.

- **Басқару серверіне мәжбүрлі қосылу үшін тарату нүктесін пайдаланыңыз**

  Егер сіз тарату нүктесі опциялары терезесінде **Осы тарату нүктесін push сервері ретінде пайдалану** параметрін таңдасаңыз, осы параметрді таңдаңыз. Әйтпесе, тарату нүктесі push серверінің рөлін атқармайды.

Байланыс профильдері ішкі бөлімінде желі орнының параметрлерін көрсетуге және басқару сервері қолжетімді болмаған кезде, автономды пайдаланушы режимін қосуға болады.

- **Желілік орналасудың параметрлері**

  Желілік орналасудың параметрлері клиент құрылғысы қосылған желінің сипаттамаларын анықтайды және желі сипаттамалары өзгерген кезде Желілік агентті бір Басқару сервері қосылымы профилінен екіншісіне ауыстыру ережелерін белгілейді.

- **Басқару серверіне қосылу профильдері**

  Бұл бөлімде Желілік агенттің Басқару серверіне қосылу профильдерін қарауға және қосуға болады. Бұл бөлімде келесі оқиғалар орын алған кезде Желілік агентті басқа Басқару серверіне ауыстыру ережелерін құрастыруға болады:

  - клиент құрылғысын басқа жергілікті желіге қосу;
  - құрылғыны ұйымның жергілікті желісінен ажырату;
  - қосылым шлюзінің мекенжайын өзгерту немесе DNS серверінің мекенжайын өзгерту.

  Қосылым профильдеріне тек Windows және macOS басқаратын құрылғылар үшін ғана қолдау көрсетіледі.

- **Басқару сервері қолжетімсіз болғанда автономды пайдаланушы режиміне ауысу**

  Параметр қосулы болса, осы профиль арқылы қосылу кезінде, клиент бағдарламасында орнатылған бағдарламалар автономды режимдегі құрылғыларға арналған саясат профильдерін және автономды пайдаланушыларға арналған саясаттарды қолданатын болады. Бағдарлама үшін автономды пайдаланушыларға арналған саясат анықталмаған болса, бағдарлама белсенді саясатты қолданатын болады.

  Параметр өшірулі болса, бағдарламалар белсенді саясаттарды қолданатын болады.

  Әдепкі бойынша, параметр өшірулі.

Байланыс кестесі бөлімінде Желілік агент деректерді Басқару серверіне жіберетін уақыт аралықтарын белгілеуге болады:

- **Қажет болғанда қосылу**

  Егер бұл нұсқа таңдалса, байланыс Желілік агент деректерді Басқару серверіне жіберуі қажет болған кезде орнатылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Көрсетілген кезеңдерде қосылу**

  Егер бұл нұсқа таңдалса, Желілік агентті Басқару серверіне қосу белгілі бір уақыт аралығында жүзеге асырылады. Бірнеше қосылу кезеңдерін қосуға болады.

Тарату нүктелері бойынша желіні сұрау

Тарату нүктелері бойынша желіні сұрау бөлімінде автоматты желі сауалнамаларын конфигурациялауға болады. Сауалнаманы қосу және оның кестесін конфигурациялау үшін келесі параметрлерді пайдалануға болады:

- **Windows желісі**

  Егер бұл параметр қосылса, Басқару сервері **Жылдам сауалнама жүргізу кестесін орнату** және **Толық сауалнама жүргізу кестесін орнату** сілтемелері бойынша конфигурацияланған кестеге сәйкес желіге автоматты түрде сауалнама жүргізеді.

  Бұл параметр өшірілсе, Басқару сервері **Желі сұрауларының жиілігі (мин)** өрісінде көрсетілген кезеңмен желіде сауалнама өткізеді.

10.2-ден төмен басқару серверіне арналған құрылғыларды анықтау уақытын **Windows домендерінен сұраулар жиілігі (мин)** (Windows желісінде жылдам сұрау жүргізу үшін) және **Желі сұрауларының жиілігі (мин)** (Windows желісінде толық сұрау жүргізу үшін) өрістерінде реттеуге болады.

Әдепкі бойынша, параметр өшірулі.

- **Zeroconf**

  Егер бұл параметр қосулы болса, тарату нүктесі автоматты түрде нөлдік конфигурациясы бар желіні (бұдан әрі *Zeroconf*) пайдалану арқылы IPv6 құрылғылары бар желіде автоматты түрде сауалнама өткізеді. Бұл жағдайда, IP ауқымдарының сауалнамасы еленбейді, өйткені тарату нүктесі бүкіл желіге сауалнама жүргізеді.

  Zeroconf пайдалануды бастау үшін келесі шарттар орындалуы керек:

  - Тарату нүктесі Linux басқаруымен жұмыс істеуі керек.
  - Тарату нүктесіне avahi-browse утилитасын орнату қажет.

  Егер бұл параметр өшірілген болса, тарату нүктесі IPv6 құрылғылары бар желілерде сауалнама жүргізбейді.

  Әдепкі бойынша, параметр өшірулі.

- **IP ауқымдары**

  Егер бұл параметр қосылса, тарату нүктесі **Сауалнама кестесін орнату** түймесі бойынша конфигурацияланған кестеге сәйкес IP ауқымына автоматты түрде сауалнама жүргізеді.

  Егер параметр өшірулі болса, тарату нүктесі IP ауқымдарының сауалнамасын өткізеді.

  10.2-ден төмен нұсқаны Желілік агент нұсқалары үшін IP ауқымдарының сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде конфигурациялауға болады. Егер параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

- **Домен контроллерлері**

  Егер бұл параметр қосылса, тарату нүктесі **Сауалнама кестесін орнату** сілтемесі бойынша конфигурацияланған кестеге сәйкес Active Directory сауалнамасын жүргізеді.

  Егер параметр өшірулі болса, Басқару сервері Active Directory сауалнамасын жүргізбейді.

  10.2-ден төмен нұсқаны Желілік агент нұсқалары үшін Active Directory сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде конфигурациялауға болады. Егер осы параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

  Опция қосылса, тарату нүктесі **Сауалнама кестесін орнату** түймесін басу арқылы конфигурацияланған кестеге сәйкес домен контроллерлеріне автоматты түрде сауалнама жүргізеді.

  Егер бұл параметр өшірулі болса, тарату нүктесі домен контроллерлеріне сауалнама жүргізбейді.

  10.2-ден төмен желілік агент нұсқалары үшін домен контроллерлері сауалнамасын өткізу мерзімділігін **Сұрау аралығы (мин)** өрісінде орнатуға болады. Егер осы параметр қосулы болса, өріс қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

Тарату нүктелерінің желі параметрлері

Егер тарату нүктелері интернетке қосылған кезде прокси-серверді пайдаланса, **Тарату нүктелерінің желі параметрлері** бөлімінде келесі параметрлерді көрсетуге болады:

- **Прокси-серверді пайдалану**
- **Мекенжай**
- **Порт нөмірі**
- **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

  Егер параметр қосулы болса, жергілікті желідегі құрылғыларға қосылған кезде прокси сервері пайдаланылмайды.

  Әдепкі бойынша, параметр өшірулі.

- **Прокси-сервердегі түпнұсқалық растама**

  Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Пайдаланушы аты**
- **Құпиясөз**

KSN Прокси (тарату нүктелері)

KSN Прокси (тарату нүктелері) бөлімінде бағдарламаны тарату нүктесі басқарылатын құрылғылардан Kaspersky Security Network (KSN) сұрауларын жіберу үшін пайдаланылатындай етіп орнатуға болады:

- **Тарату нүктесі тарапынан KSN проксиін қосу**

  KSN прокси-сервері қызметі тарату нүктесі ретінде әрекет ететін құрылғыда орындалады. Бұл параметрді желі трафигін қайта тарату және оңтайландыру үшін пайдаланыңыз.

  Тарату нүктесі Kaspersky Security Network мәлімдемесінде көрсетілген KSN статистикасын Kaspersky ұйымына жібереді.

  Әдепкі бойынша, параметр өшірулі. Осы параметрді қосу, **Басқару серверін прокси-сервер ретінде пайдалану** және **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрлері Басқару серверінің сипаттары терезесінде қосылған жағдайда ғана күшіне енеді.

  Суық резерві бар істен шығуға төзімді кластер түйініне (белсенді / пассивті) тарату нүктесін тағайындауға және сол түйінде KSN прокси-серверін қосуға болады.

- **KSN сұрауын Басқару серверіне қайта жіберу**

  Тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын Басқару серверіне жібереді.

  Әдепкі бойынша, параметр қосулы.

- **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру**

  Тарату нүктесі KSN-ге басқарылатын құрылғылардан KSN немесе KPSN бұлттық қызметіне сұраулар жібереді. Тарату нүктесінде жасалған KSN сұраулары да тікелей KSN Cloud немесе KPSN-ге жіберіледі.

  Желілік агенттің 11 (немесе одан бұрынғы) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алмайды. Тарату нүктелерін KSN сұрауларын KSN-ге жіберу үшін қайта реттегіңіз келсе, әрбір тарату нүктесі үшін **KSN сұрауын Басқару серверіне қайта жіберу** параметрін қосыңыз.

  Желілік агенттің 12 (және одан да жоғары) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алады.

- **Порт**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын TCP портының нөмірі. Әдепкі бойынша 13111-порт орнатылған.

- **UDP порты**

  Желілік агент басқару серверіне UDP порты арқылы қосылуы үшін, **UDP портын пайдалану** жалаушасын қойып, **UDP порт нөмірі** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы. Әдепкі бойынша басқару серверіне қосылу 15000 UDP порты арқылы жүзеге асырылады.

Жаңартулар (тарату нүктелері)

Жаңартулар (тарату нүктелері) бөлімінде айырмашылық файлдарын жүктеу функциясын қосуыңызға болады, себебі тарату нүктелері жаңартуларды Kaspersky жаңартулар серверлерінен айырмашылық файлдары түрінде алып тұрады.

Жергілікті есептік жазбаны басқару (тек Linux)

Жергілікті есептік жазбаны басқару (тек Linux) бөлімі үш бөлікшеден тұрады:

- **Пайдалану сертификаттарын басқару**
- **Қолданылатын жергілікті әкімші топтарын қосу не өңдеу**
- **Пайдаланушы құрылғысындағы sudoer файлдарын өзгерістерден қорғау үшін сілтемелік файл жүктеп салу**

Пайдалану сертификаттарын басқару бөлікшесінде қай түбірлік сертификаттарды орнату керектігін көрсетуге болады. Бұл сертификаттарды, мысалы, веб-сайттардың немесе веб-серверлердің түпнұсқалығын тексеру үшін пайдалануға болады.

- **Түбірлік сертификаттарды орнату**

  Бұл параметр қосылса, кестеге қосылған сертификаттар көрсетілген құрылғыларда орнатылады.

  Бұл параметр өшірілсе, сертификаттар көрсетілген құрылғыларда орнатылмайды.

  Әдепкі бойынша, параметр өшірулі.

- **Қосу**

  Бұл түймені басқан соң, сертификатты қосуға болатын терезе ашылады.

  Сертификат өлшемі 10 МБ-тан аз болуы керек.

  Kaspersky Security Center қолданбасы CER, CRT, CERT, PEM және KEY кеңейтімдері бар сертификаттарды қолдайды.

Қолданылатын жергілікті әкімші топтарын қосу не өңдеу бөлімінде жергілікті әкімші топтарын басқаруға болады. Бұл топтар, мысалы, жергілікті әкімші құқықтарын кері қайтарып алу кезінде пайдаланылады. Сондай-ақ, артықшылықты пайдаланушы есептік жазбаларының тізімін **Артықшылықтары бар құрылғы пайдаланушылары туралы есеп (тек Linux)** арқылы тексеруге болады.

- **Қосу**

  Жергілікті әкімшілер тобын қосу үшін осы түймені басыңыз.

- **Өзгерту**

  Жергілікті әкімшілер тобын өзгерту үшін осы түймені басыңыз.

  Бұл түйме жергілікті әкімшілер тобының жанында құсбелгі қойылған жағдайда қолжетімді болады.

- **Жою**

  Таңдалған жергілікті әкімшілер тобын кестеден жою үшін осы түймені басыңыз.

  Бұл түйме жергілікті әкімшілер тобының жанында құсбелгі қойылған жағдайда қолжетімді болады.

Пайдаланушы құрылғысындағы sudoer файлдарын өзгерістерден қорғау үшін сілтемелік файл жүктеп салу бөлікшесінде sudoers файлын басқаруды конфигурациялауға болады. Артықшылықтары бар топтар мен құрылғы пайдаланушылары құрылғыдағы sudoers файлы арқылы анықталады. sudoers файлы `/etc/sudoers` қалтасында орналасқан. Sudoers файлын өзгерістерден қорғау үшін sudoers анықтамалық файлын жүктеп салуға болады. Бұл sudoers файлын қажетсіз өзгертудің алдын алады.

Жарамсыз sudoers анықтамалық файлы пайдаланушы құрылғысының дұрыс жұмыс істемеуіне әкелуі мүмкін.

- **Басқаруға арналған sudoers файлы**

  Бұл параметр қосылса, sudoers файлы ағымдағы sudoers анықтамалық файлымен ауыстырылады.

  Бұл параметр өшірілсе, sudoers файлы өзгеріссіз қалады.

  Әдепкі бойынша, параметр өшірулі.

- **Сілтемелік sudoer файлы**

  Бұл өріс жүктелген sudoers анықтамалық файлының атауын көрсетеді.

- **Жүктеп салу**

  sudoers анықтамалық файлын жүктеп салу үшін осы түймені басыңыз.

- **Ағымдағы сілтемелік sudoer файлы**

  Ағымдағы sudoers файлын көру үшін осы түймені басыңыз.

Тексерістер журналы

Бұл қойыншада сіз саясатты тексеру тізімін және кері қайтарылған өзгерістерді көре аласыз.

Желілік агент саясатының параметрлерін операциялық жүйелер бойынша салыстыру

Төмендегі кестеде нақты операциялық жүйесі бар желілік агентті конфигурациялау үшін басқару консолі мен Kaspersky Security Center Web Console ішінде қандай желілік агент саясатының параметрлерін қолдануға болатыны көрсетілген.

Желілік агент саясаты параметрлері: операциялық жүйелер бойынша салыстыру

Саясаттар бөлімі	Windows	macOS	Linux
Жалпы	✓	✓	✓
Оқиғаларды конфигурациялау	✓	✓	✓
Параметрлер	✓	✓	✓ Келесі параметрлер қолжетімді: • **Файлдарды тек тарату нүктелері арқылы тарату** • **Оқиғалар кезегінің максималды өлшемі, МБ** • **Бағдарламаға құрылғыда саясаттың кеңейтілген деректерін шығарып алуға рұқсат берілген**
Қоймалар	✓	✓ **Жабдық тізімдемесі туралы ақпарат** параметрі қолжетімді.	✓ Келесі параметрлер қолжетімді: • **Орнатылған бағдарламалардың мәліметтері** • **Жабдық тізімдемесі туралы ақпарат**
Бағдарламалық жасақтаманың жаңартулары мен осалдықтары	✓	—	—
Өшіріп қайта қосуды басқару	✓	—	—
Windows компьютерлік бөлісу қызметін пайдалану	✓	—	—
Патчтарды және жаңартуларды басқару	✓	—	—
Қосылым мүмкіндігі → Желі	✓	✓	✓ **Microsoft Windows брандмауэрінде Желілік агенттің порттарын ашу** параметрлерінен басқа.
Қосылым мүмкіндігі → Байланыс профильдері	✓	✓	—
Қосылым мүмкіндігі → Байланыс кестесі	✓	✓	✓
Тарату нүктелері бойынша желіні сұрау	✓ **Windows желісі**, **IP ауқымдары** және **Домен контроллерлері** параметрлері ғана қолжетімді.	—	✓ Келесі параметрлер қолжетімді: • **Zeroconf** • **IP ауқымдары** • **Домен контроллерлері**
Тарату нүктелерінің желі параметрлері	✓	✓	✓

Саясаттар бөлімі	Windows	macOS	Linux
KSN Прокси (тарату нүктелері)	✓	—	✓
Жаңартулар (тарату нүктелері)	✓	—	✓
Тексерістер журналы	✓	✓	✓

Желілік агент үшін ресурстарды аз тұтыну режимін қосу немесе өшіру

Ресурстарды аз тұтыну режимі клиент құрылғысында орнатылған Желілік агент жедел жадын пайдалануды шектеуге мүмкіндік береді. Әдепкі бойынша, ресурстарды аз тұтыну режимі өшірілген.

Төмендегі функциялар ресурстарды аз тұтыну режимінде орындалмайды:

- Желілік агентті тарату нүктесі ретінде белгілеу мүмкін емес (қолмен немесе автоматты түрде).
- Желілік агент Желілік агенттің күйі туралы ақпаратты бөлек мәтіндік файлға жазбайды.
- Желілік агент жаңартуларды алудың офлайн-үлгісін қолдамайды.
- Келесі құрамдастар мен процестер өшірілген:
  - Үшінші тарап жаңартулары мен осалдықтары туралы ақпаратты алу.
  - KSN прокси-серверін тарату нүктесінің жағында іске қосу.
  - Тарату нүктелерінің қоймасында жаңартуларды жүктеп алу.
  - DNS серверін бұғаттауды қолданбау.
  - Дискідегі бос орын туралы ақпарат алу.

Құрамдастар мен процестер ресурстарды аз тұтыну режимі өшірілгеннен кейін өз жұмысын жалғастырады.

Ресурстарды аз тұтыну режимін қосу үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді орындаңыз:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Желілік агентті қайта іске қосыңыз.

3. Ресурстарды аз тұтыну режимі қосылғанын тексеру үшін Windows жүйесінде **Оқиғаларды қарау құралын** ашып, **Қолданбалар мен қызмет журналдары → Kaspersky Event Log оқиғалар журналы** тармағын таңдаңыз.

   Оқиғалар журналында **Kaspersky Security Center желілік агенті аз ресурстарды тұтыну режимінде жұмыс істеп тұр** деген сияқты оқиғалар бар екеніне көз жеткізіңіз.

Ресурстарды аз тұтыну режимі қосулы.

Ресурстарды аз тұтыну режимін сөндіру үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді орындаңыз:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Желілік агентті қайта іске қосыңыз.

3. Аз ресурс тұтыну режимінің өшірілгенін тексеру үшін Windows жүйесінде **Оқиғаларды қарау** құралын ашып, **Қолданбалар мен қызметтер журналдары → Kaspersky Event Log оқиғалар журналы** тармағын таңдаңыз.

   Соңғы klnagent оқиғасында **Kaspersky Security Center желілік агенті аз ресурстарды тұтыну режимінде жұмыс істеп жатыр** деген хабардың жоқ екеніне көз жеткізіңіз.

Ресурстарды аз тұтыну режимі өшірулі.

Сондай-ақ *Скриптілерді қашықтан орындау* тапсырмасының көмегімен ресурстарды аз тұтыну режимін қашықтан қосуға болады.

Басқарылатын қолданбалардың қорғаныс параметрлерін конфигурациялау

Басқарылатын Kaspersky қолданбаларының қорғаныс параметрлерін конфигурациялау үшін саясаттарды пайдалануға болады.

Kaspersky Endpoint Security саясаттарын конфигурациялау туралы қосымша ақпарат алу үшін тиісті анықтаманы қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Endpoint Security for Mac анықтамасы

Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау

Қоймаға жаңартуларды жүктеу кезінде жалаушасы қойылған кезде Kaspersky Endpoint Security **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** үшін кестенің оңтайлы және ұсынылатын нұсқасы.

Бағдарламаларды немесе бағдарламалық жасақтама жаңартуларын қашықтан жою

Қолданбаларды немесе қолданбалық жасақтама жаңартуларын қашықтан жою үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Kaspersky Security Center бағдарламасы үшін **Бағдарламаны қашықтан жою** тапсырма түрін таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.
6. Қандай қолданбаны жойғыңыз келетінін таңдаңыз, содан кейін жойғыңыз келетін қолданбаларды, жаңартуларды немесе патчтарды таңдаңыз:

   - **Басқарылатын бағдарламаны жою**

     Kaspersky бағдарламалары тізімі көрсетіледі. Жойғыңыз келетін бағдарламаны таңдаңыз.

   - **Үйлесімсіз бағдарламаны жою**

     Kaspersky немесе Kaspersky Security Center қауіпсіздік бағдарламаларына сәйкес келмейтін бағдарламалардың тізімі көрсетіледі. Жойғыңыз келетін бағдарламаларға қарама-қарсы жалаушалар қойыңыз.

   - **Бағдарламаны бағдарламалар тізімдемесінен жою**

     Әдепкі бойынша, Желілік агенттер басқарылатын құрылғыларда орнатылған бағдарламалар туралы ақпаратты Басқару серверіне жібереді. Орнатылған бағдарламалар тізімі бағдарламалар тізімдемесінде сақталады.

     Бағдарламалар тізімдемесінен бағдарламаны таңдау үшін:

     a. **Жойылатын бағдарлама** өрісіне басып, жойғыңыз келетін бағдарламаны таңдаңыз.

     Егер сіз Kaspersky Security Center Желілік агентін таңдаған болсаңыз, тапсырма басталған кезде *Сәтті түрде аяқталды* күйі жою процесінің басталғанын көрсетеді. Kaspersky Security Center Желілік агент бағдарламасын жойған кезде күй өзгермейді. Тапсырма істен шыққан жағдайда күй *Ақау* деп өзгереді.

b. Жою параметрлерін көрсетіңіз:

- **Жою режимі**

  Бағдарламаны қалай жойғыңыз келетінін таңдаңыз:

  - **Жою пәрменін автоматты түрде анықтау**

    Егер бағдарламада бағдарлама өндірушісі белгілеген жою пәрмені болса, Kaspersky Security Center бұл пәрменді пайдаланады. Осы нұсқаны таңдау ұсынылады.

  - **Жою пәрменін белгілеу**

    Бағдарламаны жою үшін пәрменіңізді көрсеткіңіз келсе, осы нұсқаны таңдаңыз.

    > Алдымен бағдарламаны **Жою пәрменін автоматты түрде анықтау** параметрімен жоюға тырысқан жөн. Егер автоматты түрде анықталған пәрменнің көмегімен жою сәтсіз болса, өз пәрменіңізді пайдаланыңыз.

    Осы өріске орнату пәрменін енгізіп, келесі параметрді көрсетіңіз:

    Әдепкі пәрмен автоматты түрде анықталмаса, әдепкі пәрменді тек жою үшін қолданыңыз

    Kaspersky Security Center бағдарламасы таңдалған бағдарламада бағдарлама өндірушісі белгілеген жою пәрмені бар-жоғын тексереді. Егер команда табылса, Kaspersky Security Center бағдарламасы оны **Бағдарламаны жою пәрмені** өрісінде көрсетілген пәрменнің орнына пайдаланады.

    Бұл параметрді қосу ұсынылады.

- **Бағдарлама сәтті жойылған соң қайта іске қосуды орындаңыз**

  Егер қолданбаны жойғаннан кейін басқарылатын құрылғыда операциялық жүйені қайта іске қосу қажет болса, операциялық жүйе автоматты түрде қайта іске қосылады.

- **Көрсетілген бағдарламаны жаңартуды, патчты немесе өзге бағдарламаны жою**

  Үшінші тарап жаңартуларының, патчтарының және бағдарламаларының тізімі көрсетіледі. Жойғыңыз келетін нысанды таңдаңыз.

  Көрсетілетін тізім, бағдарламалар мен жаңартулардың жалпы тізімі болып табылады және ол басқарылатын құрылғыларда орнатылған бағдарламалар мен жаңартуларға сәйкес келмейді. Нысанды таңдамас бұрын, тапсырманың әрекет ету ауқымында анықталған құрылғыларда бағдарламаның немесе жаңартудың орнатылғанына көз жеткізген жөн. Сипаттар терезесінде бағдарлама немесе жаңарту орнатылған құрылғылардың тізімін көруге болады.

  Құрылғылар тізімін көру үшін:

  a. Бағдарламаның немесе жаңартулардың атын басыңыз.

  Сипаттар терезесі ашылады.

  b. **Құрылғылар** бөлімін ашыңыз.

  Сондай-ақ, құрылғы сипаттары терезесінде орнатылған бағдарламалар мен жаңартулар тізімін көруге болады.

7. Клиент құрылғылары жою утилитасын қалай жүктейтінін көрсетіңіз:

- **Желілік агенттің көмегімен**

  Файлдарды клиент құрылғыларына осы клиент құрылғыларында орнатылған Желілік агент жеткізеді.

  Егер бұл параметр өшірулі болса, файлдар Microsoft Windows құралдарының көмегімен жеткізіледі.

  Егер тапсырма Желілік агенттер орнатылған құрылғыларға тағайындалса, бұл параметрді қосу ұсынылады.

- **Басқару сервері арқылы операциялық жүйе ресурстарының көмегімен**

  Файлдар Басқару серверінің операциялық жүйесінің құралдарын пайдаланып клиент құрылғыларына жіберіледі. Бұл параметрді клиент құрылғысында Желілік агент орнатылмаған, бірақ клиент құрылғысы Басқару серверімен бір желіде орналасқан кезде қосуға болады.

- **Тарату нүктелері арқылы операциялық жүйе ресурстарының көмегімен**

  Файлдар тарату нүктелері арқылы операциялық жүйенің құралдарын қолдана отырып, клиент құрылғыларына жіберіледі. Егер желіде кем дегенде бір тарату нүктесі болса, бұл параметрді қосуға болады.

  Желілік агенттің көмегімен параметрі қосылса, онда файлдар, операциялық жүйенің құралдарымен Желілік агент құралдарын пайдалану мүмкін болмаған жағдайда ғана жеткізіледі.

- **Бір уақытта орындалатын жүктеулердің ең көп саны**

  Басқару сервері файлдарды бір уақытта жібере алатын клиент құрылғыларының рұқсат етілген ең көп саны. Бұл сан неғұрлым көп болса, бағдарлама соғұрлым тезірек жойылады, бірақ Басқару серверіне жүктеме артады.

- **Жою әрекеттерінің максималды саны**

  Бағдарламаны қашықтан жою тапсырмасын іске қосу кезінде, бағдарламаны басқарылатын құрылғыдан параметрлерде көрсетілген орнатуды іске қосу саны ішінде жою мүмкін емес, Kaspersky Security Center бағдарламасы осы басқарылатын құрылғыға жою утилитасын жеткізуді тоқтатады және бұдан былай орнатушыны құрылғыда іске қоспайды.

  Жою әрекеттерінің максималды саны параметрі басқарылатын құрылғы ресурстарын сақтауға, сондай-ақ трафикті азайтуға мүмкіндік береді (жою, MSI файлын іске қосу және қате туралы хабарлар).

  Тапсырманы бірнеше рет іске қосу әрекеттері жоюға кедергі келтіретін құрылғыдағы ақаулықты көрсетуі мүмкін. Әкімші жою әрекеттерінің көрсетілген саны ішінде мәселені шешіп, тапсырманы қайта іске қосуы керек (қолмен немесе кесте бойынша).

  Егер жою орындалмаса, мәселе шешілмейтін болып саналады және кез келген кейінгі іске қосу әрекеттері ресурстар мен трафиктің қажетсіз шығыны тұрғысынан қымбат болып саналады.

  Тапсырма жасалғаннан кейін, орнату әрекеттерінің саны `0`-ге тең болады. Құрылғыдағы қатені қайталайтын әрбір орнатуды іске қосу есептегіштің көрсеткіштерін арттырады.

  Егер тапсырма параметрлерінде көрсетілген жою әрекеттерінің саны асып кетсе және құрылғы бағдарламаны жоюға дайын болса, сіз **Жою әрекеттерінің максималды саны** параметрінің мәнін арттырып, бағдарламаны жою тапсырмасын орындай аласыз. Сондай-ақ, басқа *Бағдарламаны қашықтан жою* тапсырмасын жасай аласыз.

- **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру**

  Файлдарды клиент құрылғыларына жібермес бұрын, Kaspersky Security Center бағдарламасы орнату утилитасының параметрлері клиент құрылғысының операциялық жүйесіне қолданылатындығын тексереді. Егер параметрлер қолданылмаса, Kaspersky Security Center бағдарламасы файлдарды жібермейді және бағдарламаны орнатуға тырыспайды. Мысалы, әртүрлі операциялық жүйелері бар құрылғыларды қамтитын басқару тобының құрылғыларынан кейбір бағдарламаларды орнату үшін басқару тобына орнату тапсырмасын тағайындауға болады, содан кейін қажеттіден басқа операциялық жүйесі бар құрылғыларды өткізіп жіберу үшін осы параметрді қосуға болады.

  Желілік агентті тағайындалмаған құрылғыларға қашықтан орнату кезінде Kaspersky Security Center немесе тарату нүктесі құрылғының операциялық жүйесінің түрін **Жүктеп алмас бұрын операциялық жүйенің түрін тексеру** параметріне қарамастан автоматты түрде анықтайды.

- **Жою құпиясөзін пайдалану**

  Бұл параметр, алдыңғы қадамда **Басқарылатын бағдарламаны жою** таңдалған болса және **Жойылатын бағдарлама** өрісінде Kaspersky Security Center Желілік агентін көрсетсеңіз, көрсетіледі.

  Егер бұған дейін Желілік агенттің саясат параметрлерінде Желілік агентті қашықтан жою құпиясөзін белгілеген болсаңыз, **Жою құпиясөзін пайдалану** жалаушасын қойып, **Құпиясөз** өрісіне жою құпиясөзін енгізіңіз. Желілік агентті қашықтан жою үшін құпиясөз орнатпасаңыз, жалаушаны қоймаңыз.

8. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сұрауды қайталау жиілігі (мин)**

  Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

- **Келесі уақыттан кейін қайта іске қосу (мин)**

  Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

9. Қажет болса, қашықтан жою тапсырмасын орындау үшін пайдаланылатын есептік жазбаларды қосыңыз:

   - **Есептік жазба қажет емес (Желілік агент орнатылды)**

     Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болып саналатын есептік жазбаны көрсетудің қажеті жоқ. Тапсырма, Басқару сервері қызметі жұмыс істейтін есептік жазба астында іске қосылады.

     Желілік агент клиент құрылғыларында орнатылмаған болса, бұл нұсқа қолжетімді емес.

   - **Есептік жазба қажет (Желілік агент пайдаланылмайды)**

     Егер сіз *Бағдарламаны қашықтан жою* тапсырмасын тағайындайтын құрылғыларда Желілік агент орнатылмаған болса, осы нұсқаны таңдаңыз. Бұл жағдайда қолданбаны орнату үшін пайдаланушы есептік жазбасын немесе SSH сертификатын көрсетуге болады.

     - **Жергілікті есептік жазба**. Егер бұл нұсқа таңдалса, бағдарлама инсталляторын іске қосуға негіз болатын есептік жазбаны көрсетіңіз. **Қосу** түймесін басыңыз, **Жергілікті есептік жазба** опциясын таңдаңыз және пайдаланушының есептік жазбасының деректерін көрсетіңіз.

       Тапсырма тағайындалған барлық құрылғыларда олардың ешқайсысы қажетті құқықтарға ие болмаса, бірнеше есептік жазбаны көрсетуге болады. Бұл жағдайда, тапсырманы іске қосу үшін барлық қосылған есептік жазбалар бірізді түрде, жоғарыдан төменге қарай қолданылады.

     - **SSH сертификаты**. Қолданбаны Linux басқаратын клиент құрылғысына орнатқыңыз келсе, пайдаланушы есептік жазбасының орнына SSH сертификатын көрсетуге болады. **Қосу** түймесін басыңыз, **SSH сертификаты** опциясын таңдаңыз және сертификаттың жеке және ашық кілттерін көрсетіңіз.

       Жеке кілт жасау үшін ssh-keygen утилитасын пайдалануға болады. Назар аударыңыз, Kaspersky Security Center, PEM жабық кілттері пішімін қолдайды, бірақ ssh-keygen утилитасы әдепкі бойынша OPENSSH пішіміндегі SSH кілттерін генерациялайды. OPENSSH пішімін Kaspersky Security Center қолдайды. PEM қолдау көрсетілетін пішімінде жабық кілт жасау үшін -m PEM параметрін ssh-keygen пәрменіне қосыңыз.

       Мысалы:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<пайдаланушының электрондық поштасы>"
       ```

10. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

11. **Аяқтау** түймесін басыңыз.

    Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

12. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

13. Тапсырма сипаттары терезесінде тапсырманың жалпы параметрлерін көрсетіңіз.

14. **Сақтау** түймесін басыңыз.

15. Тапсырманы қолмен іске қосыңыз немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес оның іске қосылуын күтіңіз.

Қашықтан жою тапсырмасын орындау нәтижесінде таңдалған бағдарлама таңдалған құрылғылардан жойылады.

Қашықтан жою мәселелері

Үшінші тарап қолданбаларын қашықтан жойған кезде, кейде "Қашықтан жою осы құрылғыда ескертулермен аяқталды: жойылатын қолданба орнатылмаған" деген ескертумен аяқталуы мүмкін. Бұл мәселе жойылатын қолданба әлдеқашан жойылған немесе тек жеке пайдаланушы үшін орнатылған кезде орын алады. Жеке пайдаланушы үшін орнатылған қолданбалар (бір пайдаланушыға арналған қолданбалар деп те аталады) көрінбейтін болады және пайдаланушы жүйеге кірмеген жағдайда, оларды қашықтан жою мүмкін болмайды.

Бұл әрекет бір құрылғыда бірнеше пайдаланушының қолданысына арналған қолданбалардан (бір құрылғыға арналған қолданбалар ретінде де белгілі) өзгеше. Бір құрылғыға арналған қолданбаларды құрылғының барлық пайдаланушысы көріп, пайдалана алады.

Сондықтан бір пайдаланушыға арналған қолданбаларды пайдаланушы жүйеге кірген кезде ғана жою керек.

Орнатылған қолданбалар туралы ақпарат көзі

Желілік агент Windows құрылғыларына орнатылған бағдарламалық жасақтама туралы ақпаратты келесі тіркеу кілттерінен алады:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Барлық пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Барлық пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Ағымдағы пайдаланушы үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Нақты пайдаланушылар үшін орнатылған қолданбалар туралы ақпаратты қамтиды.

Тапсырмалар

Бұл бөлімде, Kaspersky Security Center бағдарламасында қолданылатын тапсырмалар сипатталған.

Тапсырмалар туралы

Kaspersky Security Center *тапсырмаларды* құру және іске қосу арқылы құрылғыларда орнатылған Kaspersky қауіпсіздік бағдарламаларының жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Kaspersky Security Center Web Console серверінде осы бағдарлама үшін басқару плагині орнатылған жағдайда ғана Kaspersky Security Center Web Console серверінде осы бағдарлама үшін тапсырма жасай аласыз.

Тапсырмалар Басқару серверінде және құрылғыларда орындалуы мүмкін.

Басқару серверінде орындалатын тапсырмаларға мыналар жатады:

- Есептерді автоматты түрде жеткізу
- Жаңартуларды сақтау орнына жүктеу
- Басқару сервері деректерінің сақтық көшірмесін жасау
- Дерекқорларға қызмет көрсету

Құрылғыларда тапсырмалардың келесі түрлері орындалады:

- *Жергілікті тапсырмалар* – нақты құрылғыда орындалатын тапсырмалар.

  Жергілікті тапсырмаларды тек әкімші Басқару консолі арқылы ғана емес, қашықтағы құрылғының пайдаланушысы да өзгерте алады (мысалы, қауіпсіздік бағдарламасының интерфейсінде). Егер жергілікті тапсырманы басқарылатын құрылғыда әкімші де, пайдаланушы да бір уақытта өзгерткен болса, онда әкімші енгізген өзгерістер басым болып күшіне енеді.

- *Топтық тапсырмалар* – бұл аталған топтың барлық құрылғыларында орындалатын тапсырмалар.

  Егер тапсырманың сипаттарында басқаша көрсетілмесе, топтық тапсырма аталған топтың ішкі топтарына да таралады. Топтық тапсырмалар (міндетті емес) осы топқа және ішкі топтарға орналастырылған қосалқы және виртуалды Басқару серверлеріне қосылған құрылғыларда да жұмыс істейді.

- *Глобалдық тапсырмалар* – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.

Әр бағдарлама үшін сіз топтық тапсырмалардың, глобалдық тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Құрылғыдағы тапсырмаларды іске қосу тек осы тапсырмалар жасалған бағдарлама іске қосылған жағдайда ғана орындалады.

Тапсырма нәтижелері әр құрылғыдағы операциялық жүйенің оқиғалар журналында, Басқару серверіндегі оқиғалар журналында және Басқару серверінің дерекқорында сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Тапсырма аймағы

Тапсырма ауқымы — тапсырма орындалатын құрылғылар жинағы. Тапсырма ауқымының келесі түрлері бар:

- *Жергілікті тапсырма* ауқымы – құрылғының өзі.
- *Басқару серверінің тапсырмасы* ауқымы – Басқару сервері.
- *Топтық тапсырма* ауқымы – топқа кіретін құрылғылардың тізбесі.

Глобалдық тапсырма жасаған кезде оның ауқымын анықтаудың келесі әдістерін қолдануға болады:

- Қажетті құрылғыларды қолмен көрсету.

  Құрылғының мекенжайы ретінде сіз IP мекенжайын (немесе IP аралығын), NetBIOS немесе DNS атауын пайдалана аласыз.

- Құрылғылар тізімін қосылатын құрылғылар мекенжайлары тізбесін қамтитын TXT пішіміндегі файлдан құрылғылар тізімін импорттау (әр мекенжай бөлек жолда орналасуы тиіс).

  Егер құрылғылар тізімі файлдан импортталса немесе қолмен қалыптастырылса, ал құрылғылар атауы бойынша анықталса, онда тізімге ақпараты Басқару серверінің дерекқорына әлдеқашан қосылған құрылғылар ғана қосылуы мүмкін. Деректер, осы құрылғыларды қосу кезінде немесе құрылғыларды анықтау нәтижесінде дерекқорға енгізілуі тиіс.

- Құрылғы таңдауларын көрсету.

  Уақыт өте келе, тапсырманың әрекет ету ауқымы, таңдауға кіретін құрылғылардың жиынтығы қалай өзгеретіндігіне байланысты өзгеріп отырады. Құрылғыны таңдауы құрылғы атрибуттары негізінде, соның ішінде құрылғыда орнатылған бағдарламалық жасақтама негізінде, сондай-ақ құрылғыға белгіленген тегтер негізінде құрылуы мүмкін. Құрылғыны таңдауы тапсырманың әрекет ету ауқымын белгілеудің ең икемді тәсілі болып саналады.

  Құрылғы таңдаулары үшін тапсырмаларды кесте бойынша іске қосуды әрқашан Басқару сервері орындайды. Мұндай тапсырмалар Басқару серверімен байланысы жоқ құрылғыларда іске қосылмайды. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғыларда тікелей іске қосылады және құрылғы мен Басқару сервері арасындағы байланыстың болуына тәуелді емес.

Құрылғылар таңдауына арналған тапсырмалар құрылғының жергілікті уақыты бойынша емес, Басқару серверінің жергілікті уақыты бойынша іске қосылады. Әрекет ету ауқымы басқа тәсілмен белгіленетін тапсырмалар құрылғының жергілікті уақыты бойынша іске қосылады.

Тапсырманы жасау

Тапсырма жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің қадамдарын орындаңыз.
3. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
4. **Аяқтау** түймесін басыңыз.

Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

Таңдалған құрылғыларға тағайындалған тапсырманы жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.
2. Басқарылатын құрылғылар тізімінде тапсырманы іске қосу қажет құрылғылардың жанына құсбелгілерді қойыңыз. Қажетті құрылғыларды табу үшін іздеу және сүзгі функцияларын пайдалана аласыз.
3. **Тапсырманы іске қосу** түймесін басып, **Жаңа тапсырма қосу** тармағын таңдаңыз.

   Жаңа тапсырма жасау шебері іске қосылады.

   Шебердің бірінші қадамында тапсырманың әрекет ету ауқымына қосу үшін таңдалған құрылғыларды жоюға болады. Шебердің нұсқауларын орындаңыз.
4. **Аяқтау** түймесін басыңыз.

Таңдалған құрылғылар үшін тапсырма жасалды.

Тапсырманы қолмен іске қосу

Бағдарлама әр тапсырманың сипаттарында белгіленген кестеге сәйкес тапсырмаларды орындайды. Тапсырманы кез келген уақытта тапсырмалар тізімінен қолмен іске қосуға болады. Сондай-ақ, **Басқарылатын құрылғылар** тізімінен құрылғыларды таңдап, олар үшін бар тапсырманы орындауға болады.

Тапсырманы қолмен іске қосу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. Көрсетілген тапсырмалар тізімінде іске қосқыңыз келетін тапсырманың жанына жалауша қойыңыз.
3. **Іске қосу** түймесін басыңыз.

Тапсырма іске қосылды. Тапсырма күйін **Күйі** бағанында немесе **Нәтиже** түймесін басу арқылы тексере аласыз.

Тапсырмалар тізімін қарап шығу

Сіз Kaspersky Security Center бағдарламасында жасалған тапсырмалар тізімін көре аласыз.

Тапсырмалар тізімін көру үшін,

Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

Тапсырмалар тізімі көрсетіледі. Тапсырмалар, өздері қатысты болып табылатын бағдарламалардың атауы бойынша топтастырылған. Мысалы, *Бағдарламаны қашықтан жою* тапсырмасы басқару серверіне, ал *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы желілік агентке қатысты болып келеді.

Тапсырма сипаттарын көру үшін,

тапсырманың атауын басыңыз.

Тапсырма сипаттары терезесі бірнеше атаулы қойындылармен бірге көрсетіледі. Мысалы, **Тапсырма түрі** тармағы **Жалпы** қойындысында, ал тапсырма кестесі **Кесте** қойындысында көрсетіледі.

Тапсырмалардың жалпы параметрлері

Бұл бөлім көптеген тапсырмаларыңыз үшін көруге және конфигурациялауға болатын параметрлердің сипаттамасын қамтиды. Қолжетімді параметрлердің тізімі конфигурацияланатын тапсырмаға байланысты.

Тапсырманы жасау кезінде белгіленген параметрлер

Тапсырманы жасау кезінде кейбір параметрлерді белгілеуге болады. Осы параметрлердің кейбірін жасалған тапсырманың сипаттарында да өзгертуге болады.

- Операциялық жүйені қайта жүктеу параметрлері:

  - **Құрылғыны қайта іске қоспау**

    Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

  - **Құрылғыны қайта іске қосу**

    Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

  - **Пайдаланушыдан әрекетті орындауды сұрау**

    Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **Сұрауды қайталау жиілігі (мин)**

    Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

    Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

  - **Келесі уақыттан кейін қайта іске қосу (мин)**

    Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

    Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  - **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

    Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

    Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

Әдепкі бойынша, параметр өшірулі.

- Тапсырма кестесі параметрлері:

  Тапсырмаға байланысты кесте түрлері әртүрлі болуы мүмкін.

  - **Тапсырманы бастау параметрлері:**

    - **N сағат сайын**

      Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

      Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

    - **N күн сайын**

      Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

      Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

    - **N минут сайын**

      Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

      Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

    - **Апта күндері бойынша**

      Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

      Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

    - **Ай сайын**

      Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

      Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

      Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

    - **Қолмен**

      Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

      Әдепкі бойынша, осы нұсқа таңдалған.

    - **Бір рет**

      Тапсырма көрсетілген күн мен уақытта тек бір рет орындалады (тапсырманың жасалған күніне сәйкес).

- **Дереу**

  Тапсырма параметрлері сақталғаннан кейін бірден орындалады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Қоймаға жаңартуларды жүктеу кезінде**

  Бұл тапсырма жаңартуларды қоймаға жүктегеннен кейін іске қосылады. Мысалы, сізге осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін осы кесте қажет болуы мүмкін.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

- Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
- Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

  Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
- Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- Тапсырма белгіленетін құрылғыларды таңдау терезесі:

  - **Басқару серверімен анықталған желілік құрылғыларды таңдау**

    Бұл жағдайда, тапсырма арнайы құрылғыларға тағайындалады. Арнайы құрылғыларға сіз басқару топтарындағы құрылғыларды да, тағайындалмаған құрылғыларды да қоса аласыз.

    Мысалы, сіз бұл параметрді Желілік агентті тағайындалмаған құрылғыларға орнату тапсырмасында пайдалана аласыз.

- **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

  Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

  Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

- **Құрылғы таңдауына тапсырманы белгілеу**

  Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

  Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

- **Басқару тобына тапсырманы белгілеу**

  Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

  Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

  Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

- Есептік жазба параметрлері:

  - **Әдепкі бойынша есептік жазба**

    Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **Есептік жазбаны көрсету**

    Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

  - **Есептік жазба**

    Тапсырманы іске қосатын есептік жазба.

  - **Құпиясөз**

    Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

Тапсырма жасалғаннан кейін белгіленген параметрлер

Тапсырманы жасағаннан кейін ғана келесі параметрлерді белгілеуге болады.

- Топтық тапсырма параметрлері:
  - **Ішкі топтарға тарату**

    Бұл параметр тек топтық тапсырмалардың сипаттарында қолжетімді.

    Бұл параметр қосылған кезде, тапсырманың әрекет ету ауқымы мыналарды қамтиды:

    - тапсырманы жасау кезінде сіз таңдаған басқару тобы;
    - топтар иерархиясы бойынша кез келген деңгейде таңдалған басқару тобына бағынатын басқару топтары.

    Егер бұл параметр өшірулі болса, тапсырманың құрамына тапсырманы жасау кезінде таңдаған басқару тобы ғана кіреді.

    Әдепкі бойынша, параметр қосулы.

  - **Қосалқы және виртуалды Басқару серверлеріне тарату**

    Бұл параметрді қосқан кезде, негізгі Басқару серверінде жұмыс істейтін тапсырма қосалқы (соның ішінде виртуалды) Басқару серверлерінде қолданылады. Егер Қосалқы Басқару серверінде бірдей типтегі тапсырма бұрыннан бар болса, онда қосалқы Басқару серверінде екі тапсырма да қолданылады — қолданыстағы және негізгі Басқару серверінен қабыл алынған.

    Ішкі топтарға тарату параметрі қосулы болса, бұл параметр қолжетімді болады.

    Әдепкі бойынша, параметр өшірулі.

- Кестенің қосымша параметрлері:
  - **Тапсырманы бастамас бұрын, Wake-on-LAN функциясы көмегімен құрылғыларды іске қосыңыз**

    Егер жалауша қойылса, құрылғыдағы операциялық жүйе тапсырма басталғанға дейін көрсетілген уақытта жүктеледі. Әдепкі бойынша белгіленген уақыт – 5 минут.

    Тапсырманы тапсырмалар аймағындағы барлық клиент құрылғыларында, соның ішінде тапсырма басталғалы тұрған кезде өшірілген құрылғыларда орындағыңыз келсе, осы параметрді қосыңыз.

    Тапсырманы орындағаннан кейін құрылғыны автоматты түрде өшіру қажет болса, **Тапсырманы орындағаннан кейін құрылғыларды өшіру** опциясын қосыңыз. Параметр сол терезеде орналасқан.

    Әдепкі бойынша, параметр өшірулі.

  - **Тапсырманы орындағаннан кейін құрылғыларды өшіру**

    Мысалы, жұмыс уақытынан кейін жұма сайын клиент құрылғыларына жаңартуларды орнататын, содан кейін демалыс күндері сол құрылғыларды өшіретін жаңартуларды орнату тапсырмасы үшін осы параметрді қосуға болады.

    Әдепкі бойынша, параметр өшірулі.

- **Тапсырма мынанша уақыттан көбірек орындалып жатса, оны тоқтату**

  Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

  Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.

- Хабарландыру параметрлері:

  - **Тапсырмалар журналын сақтау** блогы:

    - **Басқару серверінің дерекқорында сақтау мерзімі (күндер)**

      Тапсырма аймағындағы барлық клиент құрылғыларында тапсырманы орындаумен байланысты бағдарлама оқиғалары көрсетілген күндер ішінде Басқару серверінде сақталады. Осы кезеңнен кейін ақпарат Басқару серверінен жойылады.

      Әдепкі бойынша, параметр қосулы.

    - **Құрылғыдағы ОЖ оқиғалар журналында сақтау**

      Тапсырманы орындауға байланысты, бағдарлама оқиғалары әрбір клиент құрылғысының Windows оқиғалар журналында жергілікті түрде сақталады.

      Әдепкі бойынша, параметр өшірулі.

    - **Басқару серверіндегі ОЖ оқиғалар журналында сақтау**

      Тапсырма аймағындағы барлық клиент құрылғыларында тапсырманы орындаумен байланысты бағдарлама оқиғалары Басқару серверінің операциялық жүйесінің Windows оқиғалар журналында орталықтандырылған түрде сақталады.

      Әдепкі бойынша, параметр өшірулі.

    - **Барлық оқиғаларды сақтау**

      Егер бұл параметр таңдалса, тапсырмаға қатысты оқиғалардың барлығы оқиғалар журналына жазылады.

    - **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**

      Егер бұл параметр таңдалса, оқиғалар журналына тек тапсырманы орындаумен байланысты оқиғалар жазылады.

    - **Тек тапсырманы орындау нәтижелерін сақтау**

      Егер бұл параметр таңдалса, оқиғалар журналына тек тапсырманы орындау нәтижелерімен байланысты оқиғалар жазылады.

  - **Әкімшіге тапсырманы орындау нәтижелері туралы хабарлау**

    Сіз әкімшілердің тапсырманы орындау нәтижелері туралы хабар алу жолдарын таңдай аласыз: электрондық пошта, SMS арқылы және орындалатын файлды іске қосу кезінде. Хабарландыру параметрлерін конфигурациялау үшін **Параметрлер** сілтемесі арқылы өтіңіз.

    Барлық хабарландыру тәсілдері әдепкі бойынша өшірілген.

- **Тек қателер туралы хабарлау**

  Егер бұл параметр қосылса, әкімшілер тапсырма қате аяқталған жағдайда ғана хабарландыру алады.

  Егер бұл параметр өшірулі болса, әкімшілер тапсырма аяқталғаннан кейін хабарландыру алады.

  Әдепкі бойынша, параметр қосулы.

- Қауіпсіздік параметрлері.

- Тапсырманың әрекет ету ауқымының параметрлері.

  Тапсырманың әрекет ету ауқымы қалай анықталатынына байланысты келесі параметрлер бар:

  - **Devices**

    Егер тапсырманың әрекет ету ауқымы басқару топтарымен анықталса, сіз сол топты қарай аласыз. Мұнда ешқандай өзгерістер қолжетімді емес. Алайда, сіз **Тапсырма ауқымынан шығарып тастау** конфигурациялай аласыз.

    Егер тапсырманың әрекет ету ауқымы құрылғылар тізімімен анықталса, бұл тізім құрылғыларды қосу және жою арқылы өзгертілуі мүмкін.

  - **Құрылғыны таңдау**

    Тапсырма қолданылатын құрылғылар таңдауын өзгертуге болады.

  - **Тапсырма ауқымынан шығарып тастау**

    Тапсырма қолданылмайтын құрылғылар тобын көрсетуге болады. Шығарылатын топтар тек тапсырма қолданылатын басқару тобының ішкі топтары бола алады.

- **Тексерістер журналы**.

Тапсырманы экспорттау

Kaspersky Security Center бағдарламасы тапсырманы және оның параметрлерін KLT файлына сақтауға мүмкіндік береді. Сақталған тапсырманы Kaspersky Security Center Windows, сондай-ақ Kaspersky Security Center Linux жүйелерінде импорттау үшін KLT файлын пайдалануға болады.

Тапсырманы экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. Экспорттағыңыз келетін тапсырманың жанына жалаушаны қойыңыз.

   Бір уақытта бірнеше тапсырманы экспорттауға болмайды. Бірнеше тапсырманы таңдайтын болсаңыз, **Экспорттау** түймесі белсенді емес болады. Басқару серверінің тапсырмалары да экспорттау үшін қолжетімді емес.

3. **Экспорттау** түймесін басыңыз.

4. Ашылған **Басқаша сақтау** терезесінде тапсырма файлының атауы мен жолын көрсетіңіз. **Сақтау** түймесін басыңыз.

   Басқаша сақтау терезесі Google Chrome, Microsoft Edge немесе Opera қолдансаңыз ғана көрсетіледі. Басқа браузерді қолданып жатсаңыз, тапсырма файлға автоматты түрде **Жүктеп алулар** қалтасына сақталады.

Тапсырманы импорттау

Kaspersky Security Center бағдарламасы тапсырманы KLT файлынан импорттауға мүмкіндік береді. KLT файлдында экспортталған тапсырма мен оның параметрлері бар.

Тапсырманы импорттау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Импорттау** түймесін басыңыз.
3. Импорттағыңыз келетін тапсырма файлын таңдау үшін **Шолу** түймесін басыңыз.
4. Ашылған терезеде тапсырманың KLT файлына апаратын жолды көрсетіңіз және **Ашу** түймесін басыңыз. Назар аударыңыз, сіз тек бір тапсырма файлын ғана таңдай аласыз.

   Тапсырманы өңдеу басталады.
5. Тапсырма сәтті аяқталғаннан кейін, тапсырманы тағайындағыңыз келетін құрылғыларды таңдаңыз. Бұл үшін, келесі параметрлердің бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

     Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

6. Тапсырманың әрекет ету ауқымын көрсетіңіз.

7. Импорттау тапсырмасын аяқтау үшін **Аяқтау** түймесін басыңыз.

Импорт нәтижелері бар хабарландыру пайда болады. Тапсырманы импорттау сәтті орындалса, сіз тапсырмасипаттарын қарап шығу үшін **Мәліметтер** сілтемесінен өте аласыз.

Импорт сәтті орындалғаннан кейін, тапсырма тапсырмалар тізімінде көрсетіледі. Тапсырма параметрлері мен кесте де импортталады. Тапсырма кестеге сәйкес іске қосылады.

Импортталған жаңа тапсырманың атауы бұрыннан бар тапсырманың атауымен бірдей болса, импортталған тапсырманың атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу

Жергілікті емес тапсырма үшін, сіз тапсырманы іске қосуға құқық беретін есептік жазбаны көрсете аласыз. Есептік жазбаны, тапсырманы жасау кезінде немесе қолданыстағы тапсырманың сипаттарында көрсетуге болады. Егер аталған есептік жазба ұйымда белгіленген қауіпсіздік ережелеріне сәйкес пайдаланылса, бұл ережелер есептік жазбаның құпиясөзін мезгіл-мезгіл өзгертуді талап етуі мүмкін. Есептік жазба құпиясөзінің мерзімі аяқталғаннан кейін және жаңа құпиясөзді орнатқаннан кейін, тапсырма сипаттарында жаңа жарамды құпиясөзді көрсеткенге дейін тапсырма іске қосылмайды.

Тапсырмалардың құпиясөзін өзгерту шебері, есептік жазба көрсетілген барлық тапсырмаларда ескі құпиясөзді жаңасына автоматты түрде тапсыруға мүмкіндік береді. Сондай-ақ, құпиясөзді әр тапсырманың сипаттарында қолмен өзгертуге болады.

Тапсырмалардың құпиясөзін өзгерту шеберін іске қосу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Тапсырмаларды іске қосу үшін есептік жазбалардың сәйкестендіру деректерін басқару** түймесін басыңыз.

Содан кейін, шебердің нұсқауларын орындаңыз.

1-қадам. Есептік деректерді таңдау

Сіздің жүйеңізде әрекет ететін жаңа есептік деректерді көрсетіңіз (мысалы, Active Directory жүйесінде). Шебердің келесі қадамына өткен кезде, Kaspersky Security Center бағдарламасы аталған есептік жазбаның атауы әрбір жергілікті емес тапсырманың сипаттарындағы есептік жазбаның атауына сәйкес келетіндігін тексереді. Егер есептік жазба атаулары сәйкес келсе, тапсырма сипаттарындағы құпиясөз автоматты түрде жаңасына ауысады.

Жаңа есептік жазбаны көрсету үшін келесі нұсқалардың бірін таңдаңыз:

- **Қолданыстағы есептік жазбаны пайдалану**

  Шебер, қазір Kaspersky Security Center Web Console веб-консоліне кірген есептік жазбаның атын пайдаланады. **Тапсырмаларда пайдаланылатын ағымдағы құпиясөз** өрісінде есептік жазба құпия сөзін қолмен енгізіңіз.

- **Басқа есептік жазбаны анықтау**

  Тапсырмалар іске қосылуы тиісті есептік жазбаның атын көрсетіңіз. Есептік жазбаның құпиясөзін **Тапсырмаларда пайдаланылатын ағымдағы құпиясөз** өрісінде көрсетіңіз.

Алдыңғы құпиясөз (міндетті емес; егер оны ағымдағы құпиясөзбен ауыстырғыңыз келсе) өрісін толтырған кезде, Kaspersky Security Center бағдарламасы құпиясөзді тек атауы мен ескі құпиясөз мәндері сәйкес келетін тапсырмалар үшін ауыстырады. Ауыстыру автоматты түрде орындалады. Барлық басқа жағдайларда, шебердің келесі қадамында орындалатын әрекетті таңдау керек.

2-қадам. Орындалып жатқан әрекетті таңдау

Егер шебердің бірінші қадамында сіз алдыңғы құпиясөзді көрсетпеген болсаңыз немесе көрсетілген ескі құпиясөз тапсырмалардың сипаттарында көрсетілген құпиясөздерге сәйкес келмесе, онда сіз осы тапсырмалармен орындалатын әрекетті таңдауыңыз керек.

Тапсырмамен жасалатын әрекетті таңдау үшін:

1. Әрекетті орындағыңыз келетін тапсырманың жанына жалаушаны қойыңыз.

2. Келесі әрекеттердің бірін орындаңыз:

   - Тапсырманың сипаттарында құпиясөзді жою үшін **Сәйкестендіру деректерін жою** түймесін басыңыз.

     Тапсырма әдепкі бойынша есептік жазбамен іске қосуға ауыстырып қосылған.

   - Құпиясөзді жаңасына ауыстыру үшін **Тіпті ескі құпиясөз дұрыс емес немесе берілмесе де, құпиясөзді мәжбүрлеп өзгерту** түймесін басыңыз.

   - Құпиясөзді өзгертуді болдырмау үшін **Әрекет таңдалмады** түймесін басыңыз.

Таңдалған әрекеттер шебердің келесі қадамына өткеннен кейін қолданылады.

3-қадам. Нәтижелерді қарап шығу

Шебердің соңғы қадамында анықталған тапсырмалардың әрқайсысының нәтижелерін қараңыз. Шебердің жұмысын аяқтау үшін **Аяқтау** түймесін басыңыз.

Скрипттерді қашықтан орындау тапсырмасын жасау

Клиенттік құрылғыда орнату пакетін орындау және қолданбаны қашықтан орнату үшін *Сценарийлерді қашықтан іске қосу* тапсырмасын жасауға болады.

Орнату пакетінде клиент құрылғыларында орындауға арналған скрипттер жинағы бар ZIP мұрағаты, сондай-ақ manifest.json файлы бар. Орнату пакетінің осы түрін жасау туралы қосымша ақпарат алу үшін мақаланы қараңыз.

Бұл тапсырма тек Linux үшін Желілік агенті бар құрылғыларда іске қосылуы керек.

Сценарийлерді қашықтан іске қосу тапсырмасын іске қосу үшін:

1. **Жаңа тапсырма жасау шебері** өтіңіз және **Сценарийлерді қашықтан іске қосу** тапсырма түрін таңдаңыз.
2. Тапсырманың атауын енгізіп, тапсырма тағайындалатын құрылғыларды таңдаңыз. **Келесі** түймесін басыңыз.
3. Қашықтан орындау үшін manifest.json файлы бар ZIP мұрағатына негізделген орнату пакетін таңдаңыз.

   Тапсырманы ол бұрыннан іске қосылған құрылғыларда қайта іске қосқыңыз келмесе, **Бұл тапсырманы ол ақталып қойған құрылғыларда бастамаңыз** параметрін қосыңыз.
4. Тапсырманы іске қосу үшін есептік жазбаны таңдаңыз.

   Әдепкі есептік жазбаны таңдасаңыз, тапсырманы Желілік агент (root есептік жазбасы) орындайды.

   > *Сценарийлерді қашықтан іске қосу* тапсырмасын іске қосқанда, тапсырмаға тағайындалған есептік жазбаны өзгерте алмайсыз. Тапсырма тағайындалған есептік жазбаны өзгерту үшін тапсырма параметрлерінде тапсырманы тоқтатып, қажетті есептік жазбамен тапсырманы қайта жасаңыз.
5. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
6. **Аяқтау** түймесін басыңыз.

   Скрипттерді қашықтан орындау тапсырмасы жасалды және тапсырмалар тізімінде көрсетіледі.

> *Скрипттерді қашықтан орындау* тапсырмасынан деректерді алғаннан кейін, Желілік агент тапсырма параметрлерінде көрсетілген әкімші мен пайдаланушыдан басқа барлық пайдаланушылар үшін алынған деректерге кіруді шектейді.

Скрипттерді қашықтан орындау тапсырмасын пайдаланып құрылғыларға қолданбаларды қашықтан орнату

Сценарийлерді қашықтан іске қосу тапсырмасы пайдаланушы орнату пакетін жасау арқылы клиент құрылғысында қолданбаны қашықтан орнату үшін пайдаланылуы мүмкін.

Бұл тапсырма үшін мұрағатты қалай дайындау керектігі туралы ақпаратты мақаланы қараңыз.

Клиент құрылғысында қолданбаны қашықтан орнату үшін орнату пакетін жасау үшін келесі файлдар осы тапсырма үшін жүктеп алғыңыз келетін мұрағатта болуы керек:

- `<package name>.deb`
- **install.sh**

  ```
  sudo apt-get install <пакет атауы>.deb
  ```

- **manifest.json**

  Қашықтағы қолданбаны орнатуға арналған JSON схемасы

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "< қажет болса, аргументтерді енгізіңіз >",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

  Массивтердің сипаттамасы

  1. `version` – манифест пен тапсырма файлының нұсқасы.

     Қазіргі уақытта жалғыз рұқсат етілетін мән – 1.

  2. `actions` массивінің элементтері тапсырмадағы скрипттердің құрамы мен орындалу ретін анықтайды.

     Скрипттің орындалу реті массивтегі элементтің индексіне (жайғасымына) сәйкес келеді.

  3. `actions` массивінің әрбір элементі үшін келесі элементтер анықталады.

     a. `type` – скрипттерден орындалатын пәрмен түрі. Қазіргі уақытта мән әрқашан `execute`.

     b. `path` – мұрағаттағы скрипт файлына апаратын жол.

     c. `args` – орындалатын пәрменнің бөлігі ретінде скриптке жіберілетін аргументтер.

     d. `results` – тапсырманың нәтижесіне байланысты келесі әрекеттерді анықтайтын массив.

        1. `code` – скриптті қайтаратын мән.

        2. `next` – келесі орындалатын әрекет. `continue` әрекеті келесі скриптіні орындауға жалғасады (`actions` массивіндегі элемент); `break` әрекеті тапсырманы тоқтатады.

     e. `default_next` – скрипт `results`-та жоқ мәнді қайтарса, орын алатын әрекет.

Сценарийлерді қашықтан іске қосу тапсырмасын іске қосқан кезде, Желілік агент клиент құрылғысына қолданбамен бірге орнату пакетін жүктеп алады. Клиент құрылғысы орнату пакетін алған кезде, осы құрылғыдағы Желілік агент manifest.json файлын талдайды және нәтижеге байланысты сценарийлер мен әрекеттердің орындалу ретін анықтайды, содан кейін орындауды бастайды.

Сценарийлерді қашықтан іске қосу тапсырмасы аяқталғаннан кейін қолданба клиент құрылғысына орнатылады.

Скрипттерді қашықтан орындау тапсырмасы үшін хабарландыруларды конфигурациялау және бақылау

Сценарийлерді қашықтан іске қосу тапсырмасы үшін оқиғаны сақтау кезіндегі бақылауды, жүріс-тұрысты және хабарландыруларды конфигурациялауға болады.

Сценарийлерді қашықтан іске қосу тапсырмасының күйін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

   Тапсырмалар тізімі көрсетіледі.

2. Тапсырманы таңдап, **Құрылғыдағы әрекеттер журналы** түймесін басыңыз.

   Тапсырманың орындалу барысы көрсетіледі.

Оқиғаны сақтау кезіндегі жүріс-тұрысты конфигурациялау үшін:

1. Тапсырмалар тізімінде тапсырма атын басып, **Параметрлер** қойындысына өтіңіз.
2. **Хабарландырулар** бөлімінде **Параметрлер** түймесін басыңыз.
3. Тапсырманы орындағаннан кейін, қолданба жүріс-тұрысының келесі нұсқаларының бірін таңдаңыз:
   - **Барлық оқиғаларды сақтау**.
   - **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**.
   - **Тек тапсырманы орындау нәтижелерін сақтау**.

     Оқиғалар **Құрылғыдағы әрекеттер журналы** және **Оқиғалар қоймасы** бөлімдерінде сақталады.

     Әдепкі бойынша тапсырманың нәтижелері ғана сақталады.

     > **Барлық оқиғаларды сақтау** тармағын таңдасаңыз, тапсырманың нәтижелері ғана сақталады.

4. Оқиғаларды Басқару сервері дерекқорында, Басқару серверіндегі оқиғалар журналында немесе құрылғыда сақтағыңыз келсе, сәйкес параметрді қосыңыз.

Хабарландыруларды реттеу туралы қосымша ақпарат алу үшін осы мақаланы қараңыз.

Скрипттерді қашықтан орындау тапсырмасы үшін мұрағатты дайындау

manifest.json файлына негізделген *Сценарийлерді қашықтан іске қосу* тапсырмасына арналған мұрағат келесі талаптарға сай болуы керек:

- Мұрағат пішімі: ZIP.
- Жалпы көлемі: 1 ГБ аспайды.
- Мұрағаттағы файлдар мен қалталардың саны шектелмейді.
- Мұрағаттық манифест файлы төмендегі схемаға сәйкес болуы және manifest.json деп аталуы керек. Схема құрылғыда тапсырма орындалып жатқанда ғана тексеріледі.

Манифест файлының JSON схемасы және массивтердің сипаттамасы

JSON схемасы

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
```

```
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Манифест файлының мысалы

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Мұрағат келесі құрылымға ие болуы керек:

  `manifest.json`

  `<file1>`

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

manifest.json – тапсырма манифест файлы.

<file1>, ..., <fileX> – орындалуы қажет скрипттері бар файлдар жинағы.

Манифест-файлы негізінде орнату пакетін жасау

Манифест-файлы негізінде орнату пакетін жасау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
   - Бағдарламаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.

   Басқару серверінде қолжетімді орнату пакеттерінің тізімі көрсетіледі.

2. **Қосу** түймесін басыңыз.

   Орнату пакетін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **manifest.json файлы бар ZIP мұрағаты бойынша сценарийлерді қашықтан орындау тапсырмасы үшін орнату пакетін жасаңыз** параметрін таңдаңыз.

4. Пакет атауын көрсетіңіз және **Шолу** түймесін басыңыз.

   Орнату пакетін жасау үшін файлды таңдауға болатын Windows стандартты **Ашу** терезесі ашылады.

5. Қолжетімді дискілерде орналасқан мұрағаттық файлды таңдаңыз. Бұл тапсырма үшін мұрағатты қалай дайындау керектігі туралы ақпаратты мақаланы қараңыз.

   Файл Kaspersky Security Center басқару серверіне жүктеле бастайды.

   Орнату пакетін жасау процесі басталады.

   Шебер терезесінде процестің аяқталуы туралы ақпарат көрсетіледі.

   Егер орнату пакеті жасалмаса, тиісті хабарландыру көрсетіледі.

6. Шебер терезесін жабу үшін **Аяқтау** түймесін басыңыз.

Жасалған орнату пакеті Басқару серверінің ортақ қатынасы бар қалтасының Packages салынған қалтасына жүктеледі. Жүктелгеннен кейін, орнату пакеті орнату пакеттерінің тізімінде пайда болады.

Басқару серверінде қолжетімді орнату пакеттері тізімінде, орнату пакетінің атын басу арқылы, келесі әрекеттерді орындай аласыз:

- Орнату пакетінің келесі сипаттарын қарап шыға аласыз:
  - **Атауы.** Орнату пакетінің атауы.
  - **Көзі.** Бағдарлама өндірушісінің атауы.
  - **Нұсқа.** Бағдарлама нұсқасы.
  - **Жасалған күні.** Орнату пакетін жасау күні.
  - **Өзгертілген.** Орнату пакетін өзгерту күні.
  - **Жолы.** Басқару серверіндегі пайдаланушы орнату пакетіне апаратын жол.
- Пакеттің атын және пәрмен жолының параметрлерін өзгертіңіз. Бұл функция тек Kaspersky қолданбалары негізінде жасалмаған пакеттер үшін қолжетімді.

Клиент құрылғыларын басқару

Kaspersky Security Center клиент құрылғыларын басқаруға мүмкіндік береді:

- Басқарылатын құрылғылардың, соның ішінде кластерлер мен сервер массивтерінің параметрлері мен күйлерін қарау.
- Тарату нүктелерін конфигурациялау.
- Тапсырмаларды басқару.

Басқару топтары клиент құрылғыларын бір бірлік ретінде басқаруға болатын жинаққа біріктіру үшін пайдаланылуы мүмкін. Клиент құрылғысын тек бір басқару тобына қосуға болады. Құрылғылар **Ереже шарттары** негізделген топқа автоматты түрде тағайындалуы мүмкін:

- Құрылғыны жылжыту ережелерін жасау.
- Құрылғыны жылжыту ережелерін көшіру.
- Құрылғыны жылжыту ережелеріне арналған шарттар.

Шарт бойынша құрылғыларды сүзу үшін құрылғы таңдауларын пайдалануға болады. Сондай-ақ, құрылғы таңдауларын жасау, құрылғыларды іздеу және құрылғыларды басқару топтары арасында тарату үшін құрылғыларға тегтерді тағайындауға болады.

Басқарылатын құрылғының параметрлері

Басқарылатын құрылғының параметрлерін қарап шығу үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде қажетті құрылғының атауы бар сілтемеден өтіңіз.

Таңдалған құрылғы сипаттары терезесі ашылады.

Сипаттар терезесінің жоғарғы бөлігінде параметрлердің негізгі топтарын көрсететін келесі қойындылар көрсетіледі:

- **Жалпы**

  Бұл қойындыда келесі бөлімдер бар:

  - **Жалпы** бөлімі клиент құрылғысы туралы жалпы ақпаратты қамтиды. Ақпарат, клиент құрылғысын Басқару серверімен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады:

    - **Атауы**

      Өрісте басқару тобындағы клиент құрылғысының атауын қарап шығуға және өзгертуге болады.

    - **Сипаттама**

      Өрісте клиент құрылғысының қосымша сипаттамасын енгізуге болады.

    - **Құрылғының күйі**

      Құрылғыдағы антивирустық қорғаныс күйінің және желідегі құрылғы белсенділігінің әкімші белгілеген өлшемшарттары негізінде қалыптастырылатын клиент құрылғысының күйі.

    - **Толық топ атауы**

      Құрамына клиент құрылғысы кіретін басқару тобы.

    - **Антивирустық дерекқорларды соңғы рет жаңарту уақыты**

      Құрылғыдағы антивирустық дерекқорларды немесе бағдарламаларды соңғы рет жаңарту күні.

    - **Басқару серверіне қосылған уақыты**

      Клиент құрылғысында орнатылған Желілік агентті Басқару серверіне соңғы рет қосу күні мен уақыты.

    - **Байланысқа соңғы рет шығу уақыты**

      Құрылғы соңғы рет желіде көрінген күн мен уақыт.

    - **Желілік агенттің нұсқасы**

      Орнатылған Желілік агенттің нұсқасы.

- **Жасалған күні**

  Құрылғының Kaspersky Security Center-де жасалған күні.

- **Құрылғының иесі**

  Құрылғы иесінің аты. **Құрылғы иесін басқару** сілтемесін басу арқылы пайдаланушыны құрылғы иесі ретінде тағайындауға немесе жоюға болады.

- **Басқару серверімен байланысты үзбеу**

  Осы параметрі қосулы болса, басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылым сақталады. Осындай қосылымды қамтамасыз ететін push-серверлерді қолданбасаңыз, осы параметрді қолдана аласыз.

  Егер параметр өшірулі болса және push серверлері пайдаланылмаса, басқарылатын құрылғы деректерді синхрондау немесе ақпаратты жіберу үшін Басқару серверіне қосылады.

  Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың жалпы саны 300-ден аспауы тиіс.

  Бұл параметр басқарылатын құрылғыларда әдепкі бойынша өшіріледі. Бұл параметр Басқару сервері орнатылған құрылғыда әдепкі бойынша қосылады және оны өшіруге тырыссаңыз да қосулы қалады.

- **Желі** бөлімінде клиент құрылғысының желілік сипаттары туралы келесі ақпарат көрсетіледі:

  - **IP мекенжайы**

    Құрылғының IP мекенжайы.

  - **Windows домені**

    Windows домені немесе құрылғы кіретін жұмыс тобы.

  - **DNS атауы**

    Клиент құрылғысының DNS домен атауы.

  - **NetBIOS атауы**

    Windows желісіндегі клиент құрылғысының атауы.

  - **IPv6 мекенжайы**

- **Жүйе** бөлімінде клиент құрылғысында орнатылған операциялық жүйе туралы ақпарат ұсынылған:

  - **Операциялық жүйе**

  - **Орталық процессор құрылымы**

  - **Құрылғы атауы**

  - **Виртуалды машинаның түрі**

    Виртуалды машинаның өндірушісі

  - **VDI бөлігі ретінде динамикалық виртуалды машина**

Бұл жолда клиент құрылғысының VDI бөлігі ретінде динамикалық виртуалды машина екені көрсетілген.

- **Қорғаныс** бөлімінде клиент құрылғысында антивирустық қорғаныстың күйі туралы келесі ақпарат ұсынылған:
  - **Көзге көрінетін**

    Клиенттік құрылғының көріну күйі.
  - **Құрылғының күйі**

    Құрылғыдағы антивирустық қорғаныс күйінің және желідегі құрылғы белсенділігінің әкімші белгілеген өлшемшарттары негізінде қалыптастырылатын клиент құрылғысының күйі.
  - **Күйдің сипаттамасы**

    Клиент құрылғысының қорғаныс күйі және Басқару серверіне қосылу.
  - **Қорғаныс күйі**

    Клиент құрылғысынның тұрақты қорғанысының ағымдағы күйі.

    Құрылғыда күй өзгергеннен кейін, жаңа күй, клиент құрылғысы Басқару серверімен синхрондалғаннан кейін ғана құрылғының сипаттары терезесінде көрсетіледі.
  - **Соңғы рет толық сканерлеу уақыты**

    Клиент құрылғысында зиянды БҚ соңғы іздеу күні мен уақыты.
  - **Вирус анықталды**

    Қауіпсіздік бағдарламасын орнатқан сәттен бастап (құрылғыны бірінші рет тексеру) немесе қауіп есептегіші соңғы нөлденген сәттен бастап клиент құрылғысында анықталған қауіптердің жалпы саны.
  - **Зарарсыздандырудан өтпеген нысандар**

    Клиент құрылғысындағы кейін өңделетін файлдар саны.

    Өрісте ұялы құрылғылар үшін кейін өңделетін файлдар ескерілмейді.
  - **Дискілерді шифрлау күйі**

    Құрылғының жергілікті дискілеріндегі файлдарды шифрлаудың ағымдағы күйі. Күйдің сипаттамасы Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.
- **Бағдарлама анықтаған құрылғы күйі** бөлімінде клиент құрылғысында орнатылған басқарылатын бағдарлама анықтаған құрылғының күйі туралы ақпарат көрсетіледі. Құрылғының бұл күйі Kaspersky Security Center анықтағаннан өзгеше болуы мүмкін.

- **Бағдарламалар**

  Бұл қойындыда клиенттік құрылғыда орнатылған барлық Kaspersky қолданбасының тізімі берілген. Бұл қойындыда таңдалған Kaspersky қолданбасын (желілік агенттен басқа) іске қосуға және тоқтатуға мүмкіндік беретін **Іске қосу** және **Тоқтату** түймелері бар. Әкімшілік серверімен байланыс сұрауларын алу үшін басқарылатын құрылғыларда 15000 UDP порты қолжетімді болса, бұл түймелерді пайдалануға болады. Басқарылатын құрылғы push хабарландырулары үшін қолжетімді болмаса, бірақ Басқару серверіне тұрақты қосылу режимі қосылған болса (**Жалпы Басқару серверімен байланысты үзбеу** параметрі қосылған), **Іске қосу** және **Тоқтату** түймелері белсенді болады. Әйтпесе, бағдарламаны іске қосу немесе тоқтату әрекеті кезінде қате туралы хабар пайда болады. Бағдарлама туралы жалпы ақпаратты, құрылғыда болған оқиғалар тізімін және бағдарлама параметрлерін көру үшін бағдарлама атауын басуға да болады.

- **Белсенді саясаттар мен профильдері**

  Осы қойындыда басқарылатын құрылғыға тағайындалған саясат тізімдері мен саясат профильдері көрсетіледі.

- **Тапсырмалар**

  Тапсырмалар қойыншасында сіз клиент құрылғысының тапсырмаларын басқара аласыз: қолданыстағы тапсырмалар тізімін қарау, жаңаларын жасау, тапсырмаларды жою, іске қосу және тоқтату, олардың параметрлерін өзгерту және орындалу нәтижелерін қарау. Тапсырмалар тізімі клиентті Басқару серверімен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады. Тапсырмалардың күйі туралы ақпаратты клиент құрылғысынан Басқару сервері сұрайды. Егер UDP порты 15000 Басқарылатын құрылғыларда Әкімшілік серверімен байланыс сұрауларын қабылдау үшін қол жетімді болса, тапсырма күйі көрсетіледі және тапсырмаларды басқару түймелері белсенді болады. Егер push-сервер басқарылатын құрылғымен байланыса алмаса, бірақ Басқару серверіне тұрақты қосылу режимі қосылған болса (**Басқару серверімен байланысты үзбеу** параметрі **Жалпы** бөлімінде қосылған), тапсырмалары бар әрекеттер қол жетімді.

  Байланыс болмаған жағдайда, күй көрсетілмейді.

- **Оқиғалар**

  Оқиғалар қойыншасында таңдалған клиент құрылғысы үшін Басқару серверінде тіркелген оқиғалар көрсетіледі.

  Құрылғылар оқиғаларын экспорттауға, көшіруге және жоюға болады.

- **Қауіпсіздік мәселелері**

  Қауіпсіздік мәселелері қойындысында клиенттік құрылғы үшін қауіпсіздік мәселелерін көруге, өңдеуге және жасауға болады. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін. Мысалы, кейбір пайдаланушылар зиянды бағдарламаны алынбалы жетектерден құрылғыларға жүйелі түрде жылжытса, әкімші қауіпсіздік мәселесін жасай алады. Әкімші қауіпсіздік мәселесі мәтінінде пайдаланушыға қарсы жасалуы керек жағдай мен ұсынылған әрекеттердің қысқаша сипаттамасын (мысалы, тәртіптік іс-әрекеттер) көрсете алады және пайдаланушыға не пайдаланушыларға сілтеме қоса алады.

  Қажетті әрекеттер орындалған қауіпсіздік мәселесі *өңделген* деп аталады. Өңделмеген қауіпсіздік мәселелерінің болуы құрылғының күйін *Критикалық* немесе *Ескерту* күйіне өзгерту шарты ретінде таңдалуы мүмкін.

  Бөлімде құрылғы үшін жасалған қауіпсіздік мәселелерінің тізімі берілген. Қауіпсіздік мәселелері маңыздылық деңгейі мен түріне қарай жіктеледі. Қауіпсіздік мәселесінің түрі қауіпсіздік мәселесін жасайтын Kaspersky қолданбасы арқылы анықталады. Өңделген қауіпсіздік мәселелерін **Өңделген** бағанына жалауша қою арқылы тізімде белгілеуге болады.

- **Тегтер**

  Тегтер қойыншасында клиент құрылғысын іздеуге негізделген кілт сөздер тізімін басқаруға болады: қолданыстағы тегтер тізімін қарау, тізімнен тегтер тағайындау, автоматты түрде тег қою ережелерін конфигурациялау, жаңа тегтер қосу және ескі тегтердің атын өзгерту, тегтерді жою.

- **Кеңейтілген**

  Бұл қойындыда келесі бөлімдер бар:

  - **Бағдарламалар тізімдемесі**. Осы бөлімде клиент құрылғысында орнатылған бағдарламалар мен оларға арналған жаңартулардың тізімдемесін көруге, сондай-ақ бағдарламалар тізімдемесінің көрсетілуін конфигурациялауға болады.

    Орнатылған бағдарламалар туралы ақпарат, клиент құрылғысында орнатылған Желілік агент қажетті ақпаратты Басқару серверіне берген жағдайда беріледі. Басқару серверіне ақпаратты беру параметрлерін **Қоймалар** бөліміндегі Желілік агент сипаттары немесе оның саясаты конфигурациялауға болады.

    Бағдарлама атауын басқан кезде бағдарлама туралы мәліметтері және сол бағдарлама үшін орнатылған жаңарту пакеттерінің тізімі бар терезе ашылады.

  - **Орындалатын файлдар**. Осы бөлімде клиент құрылғысында табылған орындалатын файлдар көрсетіледі.

  - **Тарату нүктелері**. Бұл бөлімде құрылғы өзара әрекеттесетін тарату нүктелерінің тізімі берілген.

    - **Файлға экспортталуда**

      Файлға экспорттау түймесі арқылы сіз құрылғы өзара әрекеттесетін тарату нүктелерінің тізімін файлға сақтай аласыз. Әдепкі бойынша, бағдарлама құрылғылар тізімін CSV пішіміндегі файлға экспорттайды.

    - **Сипаттар**

      Сипаттар түймесі арқылы құрылғы өзара әрекеттесетін тарату нүктесінің параметрлерін көруге және конфигурациялауға болады.

  - **Жабдық тізімдемесі**. Осы бөлімде клиент құрылғысында орнатылған жабдық туралы ақпаратты көруге болады.

    Желілік агент Windows жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді:

    - ЖЖҚ
    - Жаппай сақтау құрылғылары
    - Негізгі тақта
    - Процессор
    - Желілік адаптерлер
    - Мониторлар
    - Бейне адаптері
    - Дыбыстық карта

Желілік агент Linux немесе macOS жүйесімен жұмыс істейтін құрылғыға орнатылған болса, ол басқару серверіне құрылғының аппараттық жасақтамасы туралы келесі ақпаратты жібереді (бұл ақпаратты операциялық жүйе қамтамасыз етсе):

- Жалпы ЖЖҚ көлемі
- Жаппай сақтау құрылғыларының жалпы көлемі
- Негізгі тақта
- Процессор
- Желілік адаптерлер

- **Қолжетімді жаңартулар**. Бұл бөлімде құрылғыда орнатылмаған бағдарламалық жасақтама жаңартуларының тізімін көруге болады.

- **Бағдарламалық жасақтама осалдықтары**. Осы бөлімде клиент құрылғыларында орнатылған үшінші тарап бағдарламаларының осалдығы туралы ақпарат бар тізімді көруге болады.

  Осалдықтарды файлға сақтау үшін, сақтағыңыз келетін осалдықтардың жанына жалаушалар қойып, **CSV файлына экспорттау** түймесін немесе **TXT файлына экспорттау** түймесін басыңыз.

  Осы бөлім келесі параметрлерді қамтиды:

  - **Тек түзетуге болатын осалдықтарды көрсету**

    Егер параметр қосулы болса, бөлімде патчпен жабуға болатын осалдықтар көрсетіледі.

    Параметр өшірулі болса, бөлімде патчпен жабуға болатын осалдықтар да, патч жоқ осалдықтар да көрсетіледі.

    Әдепкі бойынша, параметр қосулы.

  - **Осалдықтың сипаттары**

    Бағдарламаларда таңдалған осалдықтың сипаттарын бөлек терезеде көру үшін тізімдегі бағдарламалардағы осалдықтың атын басыңыз. Сипаттар терезесінде келесі әрекеттерді орындауға болады:

    - Осы басқарылатын құрылғыдағы бағдарламаларда (Басқару консолінде немесе Kaspersky Security Center Web Console веб-консолінде) осалдықты өткізіп жіберу.
    - Осалдық үшін ұсынылған түзетулер тізімін қарап шығу.
    - Осалдықты түзету үшін бағдарламалық жасақтама жаңартуын қолмен көрсету (Басқару консолінде немесе Kaspersky Security Center Web Console веб-консолінде).
    - Осалдықтардың даналарын қарап шығу.
    - Осалдықты жабу үшін бар тапсырмалар тізімін қарап шығу және осалдықты жабу үшін тапсырмалар жасау.

- **Қашықтан диагностикалау**. Бұл бөлімде клиент құрылғыларын қашықтан диагностикалауға болады.

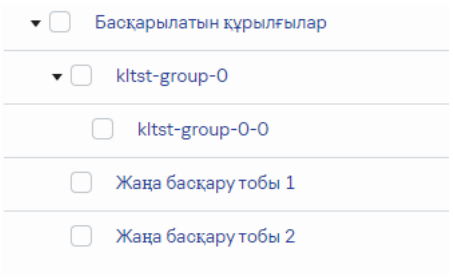
PostgreSQL, MariaDB немесе MySQL ДҚБЖ пайдалансаңыз, **Оқиғалар** қойындысы таңдалған клиент құрылғысы үшін оқиғалардың толық тізімін көрсетпеуі мүмкін. Бұл, ДҚБЖ оқиғалардың өте көп санын сақтаған кезде орын алады. Келесі әрекеттердің бірін орындау арқылы көрсетілетін оқиғалар санын көбейтуге болады:

- Керек емес оқиғаларды жою.
- Керек емес оқиғаларды сақтау мерзімін қысқарту.

Құрылғы үшін Басқару серверінде тіркелген оқиғалардың толық тізімін көру үшін Есептерді пайдаланыңыз.

Басқару топтарын жасау

Kaspersky Security Center орнатылғаннан кейін бірден басқару топтарының иерархиясында бір ғана Басқару тобы бар – **Басқарылатын құрылғылар**. Басқару топтарының иерархиясын құру кезінде **Басқарылатын құрылғылар** қалтасына құрылғылар мен виртуалды машиналарды қосып, салынған топтарды қосуға болады (төмендегі суретті қараңыз).



Басқару топтарының иерархиясын қарау

Басқару тобын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Басқару тобының құрылымында жаңа басқару тобы кіруі тиісті топқа сәйкес келетін салынған қалтаны таңдаңыз.
3. **Қосу** түймесін басыңыз.
4. Ашылған **Жаңа басқару тобының аты** терезесінде топтың атауын енгізіп, **Қосу** түймесін басыңыз.

Нәтижесінде, басқару топтарының иерархиясында атауы көрсетілген жаңа басқару тобы пайда болады.

Бағдарлама Active Directory құрылымына немесе домендік желі құрылымына негізделген басқару топтарының құрылымын құруға мүмкіндік береді. Сондай-ақ, мәтіндік файлдан топтар құрылымын жасауға болады.

Басқару топтарының құрылымын құру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. **Импорттау** түймесін басыңыз.

Нәтижесінде, басқару топтарының құрылымын жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

Басқару тобы құрамына құрылғыларды қолмен қосу

Құрылғыларды жылжыту ережелерін жасау арқылы немесе құрылғыларды бір басқару тобынан екіншісіне жылжыту арқылы немесе құрылғыларды таңдалған басқару тобына қосу арқылы құрылғыларды автоматты түрде басқару топтарына жылжытуға болады. Бұл бөлімде құрылғыларды басқару тобына қолмен қосу тәсілі сипатталған.

Таңдалған басқару тобына бір немесе бірнеше құрылғыны қолмен қосу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Тізімнің үстіндегі **Ағымдағы жол**: `<current path>` сілтемесінен өтіңіз.
3. Ашылған терезеде құрылғыларды қосуды қажет ететін басқару тобын таңдаңыз.
4. **Құрылғылар қосу** түймесін басыңыз.

   Нәтижесінде, құрылғыларды жылжыту шебері іске қосылады.
5. Басқару тобына қосқыңыз келетін құрылғылардың тізімін құрастырыңыз.

   > Құрылғылар тізіміне құрылғыны қосқан кезде немесе құрылғыларды табу нәтижесінде Басқару сервері дерекқорына ақпарат қосылған құрылғыларды ғана қосуға болады.

   Тізімге құрылғыларды қалай қосқыңыз келетінін таңдаңыз:

   - **Құрылғылар қосу** түймесін басып, құрылғыларды келесі тәсілдердің бірімен көрсетіңіз:
     - Басқару сервері анықтаған құрылғылар тізімінен құрылғыларды таңдаңыз.
     - Құрылғылардың IP мекенжайларын немесе IP ауқымын көрсетіңіз.

       > IP ауқымында 1,048,576 IPS мекенжайынан артық болмауы керек.

     - NetBIOS құрылғы атауын немесе DNS атауын көрсетіңіз.

       > Құрылғы атауы бар өрісте бос орындар, сондай-ақ келесі тыйым салынған таңбалар болмауы керек: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
   - Құрылғыларды TXT пішіміндегі файлдан импорттау үшін **Құрылғыларды файлдан импорттау** түймесін басыңыз. Әрбір құрылғы мекенжайы (немесе құрылғы атауы) бөлек жолда орналасуы тиіс.

     > Файлда бос орындар, сондай-ақ келесі тыйым салынған таңбалар болмауы керек: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Басқару тобына қосылатын құрылғылар тізімін қараңыз. Сіз құрылғыларды қосу немесе жою арқылы тізімді өңдей аласыз.

7. Тізімде қателердің жоқ екеніне көз жеткізгеннен кейін, **Келесі** түймесін басыңыз.

Шебер құрылғылар тізімін өңдеп, нәтижені көрсетеді. Шебер аяқталғаннан кейін, таңдалған құрылғылар басқару тобының құрамына енеді және олар үшін Басқару сервері берген атаулары бар құрылғылар тізімінде көрсетіледі.

Құрылғыларды немесе кластерлерді басқару тобының құрамына қолмен жылжыту

Құрылғыларды бір басқару тобынан екіншісіне немесе тағайындалмаған құрылғылар тобынан басқару тобына жылжытуға болады.

Сондай-ақ кластерлерді немесе серверлер массивтерін бір басқару топтан екіншісіне жылжытуға болады. Кластерді немесе серверлер массивін басқа топқа жылжытқанда, оның барлық түйіндері онымен бірге жылжытылады, өйткені кластер және оның кез келген түйіні әрқашан бір басқару топқа жатады. **Құрылғылар** қойындысында бір кластер түйінін таңдаған кезде **Топқа жылжыту** түймесі қолжетімсіз болады.

Таңдалған басқару топ құрамына бір немесе бірнеше құрылғыны немесе кластерді жылжыту үшін:

1. Құрылғыларды жылжытқыңыз келетін басқару тобын ашыңыз. Ол үшін келесі әрекеттердің бірін орындаңыз:

   - Басқару тобын ашу үшін негізгі мәзірде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** тармағына өтіп, **Ағымдағы жол** өрісіндегі жол сілтемесін басыңыз және ашылатын сол жақ панельден басқару тобын таңдаңыз.

   - **Тағайындалмаған құрылғылар** тобын ашу үшін негізгі мәзірде **Табу және орналастыру** → **Тағайындалмаған құрылғылар** бөліміне өтіңіз.

2. Басқару топта кластерлер немесе сервер массивтері болса, **Басқарылатын құрылғылар** бөлімі екі қойындыға бөлінеді – **Құрылғылар** және **Кластерлер және серверлердің массивтері**. Жылжытқыңыз келетін нысанның қойындысын ашыңыз.

3. Басқа топқа жылжыту қажет құрылғылардың немесе кластерлердің жанындағы жалаушаларды белгілеңіз.

4. **Топқа жылжыту** түймесін басыңыз.

5. Басқару топтардың иерархиясында таңдалған құрылғыларды немесе кластерлерді жылжытқыңыз келетін Басқару топтың жанындағы жалаушаларды белгілеңіз.

6. **Жылжыту** түймесін басыңыз.

Таңдалған құрылғылар немесе кластерлер таңдалған басқару топқа жылжытылады.

Құрылғыны жылжыту ережелерін жасау

Құрылғыларды басқару топтары бойынша таратылатын құрылғыны жылжыту ережелерін конфигурациялауға болады.

Құрылғыны жылжыту ережесін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Жылжыту ережелері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Ашылған терезеде, **Жалпы** қойыншасында келесі деректерді көрсетіңіз:
   - **Ереженің атауы**

     Жаңа белсендіру ережесінің атын көрсетіңіз.

     Егер сіз ережені көшірсеңіз, жаңа ереже бастапқы ережемен бірдей атау алады, бірақ оған жақшаға индекс қосылады, мысалы: (1).

   - **Басқару тобы**

     Құрылғылар автоматты түрде жылжытылатын басқару тобын таңдаңыз.

   - **Белсенді ереже**

     Егер бұл параметр қосылса, ереже қосылады және сақталғаннан кейін бірден қолданыла бастайды.

     Егер бұл параметр өшірулі болса, ереже жасалады, бірақ ол қосылмайды. Бұл параметрді өшірмейінше, ереже жұмыс істемейді.

   - **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту**

     Егер бұл параметр қосулы болса, тек тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

     Егер бұл параметр өшірулі болса, басқа басқару топтарына жататын құрылғылар, сондай-ақ тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

   - **Ережені қолдану**

     Сіз келесі нұсқаның бірін таңдай аласыз:
     - **Әр құрылғыға бір реттен іске қосу**

       Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады.

     - **Әр құрылғыға бір реттен іске қосу, одан кейін әр Желілік агентке қайта орнатқан сайын іске қосу**

       Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады, содан кейін сол құрылғыларда Желілік агент қайта орнатылған кезде ғана қолданылады.

     - **Ережені үздіксіз қолдану**

       Ереже Басқару серверде автоматты түрде орнатылатын кестеге сәйкес қолданылады (әдетте бірнеше сағат сайын).
4. **Ереже шарттары** қойыншасында құрылғылар басқару тобына жылжытылатын кемінде бір өлшемшартті көрсетіңіз.
5. **Сақтау** түймесін басыңыз.

Жылжыту ережесі жасалады. Ол жылжыту ережелерінің тізімінде пайда болады.

Тізімдегі ереже неғұрлым жоғары болса, оның басымдығы да соғұрлым жоғары болады. Жылжыту ережесінің басымдылығын арттыру немесе азайту үшін ережені сәйкесінше тізімде жоғары немесе төмен жылжыту үшін тінтуірді пайдаланыңыз.

Ережені үздіксіз қолдану параметрі таңдалса, жылжыту ережесі басымдыққа қарамастан қолданылады. Мұндай ережелер Басқару сервері автоматты түрде орнататын кестеге сәйкес қолданылады.

Егер құрылғының атрибуттары бірден бірнеше ережеге сай келсе, онда құрылғы үлкен басымдыққа ие ереженің мақсатты тобына көшіріледі (ережелер тізімінде жоғары тұр).

Құрылғыны жылжыту ережелерін көшіру

Құрылғыларды жылжыту ережелерін көшіруге болады, мысалы, әртүрлі мақсатты басқару топтары үшін бірнеше бірдей ереже керек болса.

Құрылғыны жылжыту ережесін көшіру үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Жылжыту ережелері** бөліміне өтіңіз.
   - Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Жылжыту ережелері** бөліміне өтіңіз.

   Құрылғыларды жылжыту ережелерінің тізімі көрсетіледі.

2. Көшіре қажет ережеге қарама-қарсы жалауша қойыңыз.

3. **Көшіру** түймесін басыңыз.

4. Ашылған терезеде, қажет болса **Жалпы** қойыншасындағы деректерді өзгертіңіз немесе параметрлерді өзгертпей, тек ережені көшіре қажет болса, қолданыстағы мәндерді қалдырыңыз:

   - **Ереженің атауы**

     Жаңа белсендіру ережесінің атын көрсетіңіз.

     Егер сіз ережені көшірсеңіз, жаңа ереже бастапқы ережемен бірдей атау алады, бірақ оған жақшаға индекс қосылады, мысалы: (1).

   - **Басқару тобы**

     Құрылғылар автоматты түрде жылжытылатын басқару тобын таңдаңыз.

   - **Белсенді ереже**

     Егер бұл параметр қосылса, ереже қосылады және сақталғаннан кейін бірден қолданыла бастайды.

     Егер бұл параметр өшірулі болса, ереже жасалады, бірақ ол қосылмайды. Бұл параметрді өшірмейінше, ереже жұмыс істемейді.

   - **Тек басқару тобында орналастырылмаған құрылғыларды жылжыту**

     Егер бұл параметр қосулы болса, тек тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

     Егер бұл параметр өшірулі болса, басқа басқару топтарына жататын құрылғылар, сондай-ақ тағайындалмаған құрылғылар таңдалған топқа көшіріледі.

- **Ережені қолдану**

  Сіз келесі нұсқаның бірін таңдай аласыз:

  - **Әр құрылғыға бір реттен іске қосу**

    Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады.

  - **Әр құрылғыға бір реттен іске қосу, одан кейін әр Желілік агентке қайта орнатқан сайын іске қосу**

    Ереже көрсетілген өлшемшарттарға сәйкес келетін әрбір құрылғы үшін бір рет қолданылады, содан кейін сол құрылғыларда Желілік агент қайта орнатылған кезде ғана қолданылады.

  - **Ережені үздіксіз қолдану**

    Ереже Басқару серверде автоматты түрде орнатылатын кестеге сәйкес қолданылады (әдетте бірнеше сағат сайын).

5. **Ереже шарттары** қойыншасында автоматты түрде жылжыту қажет құрылғылар үшін өлшемшарттарды көрсетіңіз.

6. **Сақтау** түймесін басыңыз.

Жаңа жылжыту ережесі жасалады. Ол жылжыту ережелерінің тізімінде пайда болады.

Құрылғыны жылжыту ережелеріне арналған шарттар

Клиент құрылғыларын басқару топтарына жылжыту ережелерін жасау немесе көшіру кезінде, **Ереже шарттары** қойыншасында құрылғыларды жылжыту шарттарын жасайсыз. Қандай құрылғыларды жылжыту керектігін анықтау үшін келесі критерийлерді қолдануға болады:

- Клиент құрылғыларына берілген тегтер.
- Желі параметрлері. Мысалы, IP мекенжайлары бар құрылғыларды көрсетілген ауқымнан жылжытуға болады.
- Желілік агент немесе Басқару сервері сияқты клиент құрылғыларында орнатылған басқарылатын бағдарламалар.
- Клиент құрылғылары болып табылатын виртуалды машиналар.
- Клиент құрылғылары бар Active Directory (OU) еншілес бөлімшелері туралы ақпарат.
- Клиент құрылғылары бар бұлттық сегмент туралы ақпарат.

Төменде, сіз бұл ақпаратты құрылғыларды жылжыту ережесінде қалай көрсету керектігі туралы сипаттама таба аласыз.

Ережеде бірнеше шарттар көрсетілсе, AND логикалық операторы іске қосылады және барлық шарттар бір уақытта қолданылады. Егер сіз қандай да бір параметрлерді таңдамасаңыз немесе кейбір өрістерді бос қалдырсаңыз, мұндай шарттар қолданылмайды.

Тегтер қойыншасы

Бұл қойыншада бұған дейін клиент құрылғыларының сипаттамаларына қосылған кілт сөздер (тегтер) бойынша құрылғыларды іздеуді конфигурациялауға болады. Бұл үшін қажетті тегтерді таңдаңыз. Сонымен қатар, сіз келесі параметрлерді қосуға болады:

- **Көрсетілген тегтерсіз құрылғыларға қолдану**

  Сипаттамада таңдалған тегі бар бағдарламалар орнатылған барлық құрылғылар құрылғылар таңдауына қосылады. Егер бұл параметр өшірулі болса, құрылғыларды жылжыту ережесі барлық таңдалған тегтері бар құрылғыларға қолданылады.

  Әдепкі бойынша, параметр өшірулі.

- **Кем дегенде бір көрсетілген тег сәйкес келген жағдайда қолдану**

  Егер бұл параметр қосулы болса, құрылғыларды жылжыту ережесі таңдалған тегтердің кем дегенде біреуі бар клиент құрылғыларына қолданылады. Егер бұл параметр өшірулі болса, құрылғыларды жылжыту ережесі барлық таңдалған тегтері бар құрылғыларға қолданылады.

  Әдепкі бойынша, параметр өшірулі.

Желі қойыншасы

Бұл қойыншада құрылғыларды жылжыту ережесін ескеретін құрылғылардың желілік деректерін көрсетуге болады:

- **Windows желісіндегі құрылғының атауы**

  Windows желісіндегі құрылғы атауы (NetBIOS атауы) немесе IPv4 мекенжайы не IPv6 мекенжайы.

- **Windows домені**

  Құрылғыларды жылжыту ережесі көрсетілген Windows доменіне қосылған барлық құрылғыларға қолданылады.

- **Құрылғының DNS аты**

  Жылжытқыңыз келетін клиент құрылғысының доменінің DNS атауы. Желіңізде DNS сервері болса, осы өрісті толтырыңыз.

  > Kaspersky Security Center үшін пайдаланып жатқан дерекқорда тіркелімді ескере отырып сұрыптау конфигурацияланған болса, құрылғының DNS атауын көрсеткенде тіркемді ескеріңіз. Әйтпесе, құрылғыны көшіру ережесі жұмыс істемейді.

- **DNS домені**

  Құрылғыларды жылжыту ережесі көрсетілген негізгі DNS суффиксіне қосылған барлық құрылғыларға қолданылады. Желіңізде DNS сервері болса, осы өрісті толтырыңыз.

- **IP ауқымы**

  Бұл параметр қосулы болса, енгізу өрістерінде сіз іздеген құрылғылар кіруі тиісті аралықтың бастапқы және соңғы IP мекенжайларын көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Басқару серверіне қосылуға арналған IP мекенжайы**

  Егер бұл параметр қосылса, клиент құрылғылары Басқару серверіне қосылатын IP мекенжайларын белгілеуге болады. Бұл үшін, барлық қажетті IP мекенжайларын қамтитын IP ауқымын көрсетіңіз.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы мына IP ауқымында орналасқан**

  Бұл опция қосылса, **IP ауқымдары** бөлімінде бұдан алдын таңдалған IP ауқымын таңдай аласыз. Таңдалған IP ауқымында тиісті құрылғылар қамтылуы керек.

  Әдепкі бойынша, параметр өшірулі.

- **Байланыс профилі өзгертілді**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек қосылым профилі өзгертілген клиент құрылғыларына қатысты қолданылады.
  - **Жоқ**. Құрылғыларды жылжыту ережесі байланыс профилі өзгермеген клиенттік құрылғыларға ғана қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **Басқа Басқару серверімен басқарылады**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек басқа Басқару серверлері басқаратын клиент құрылғыларына қолданылады. Бұл Серверлер құрылғыларды жылжыту ережесін конфигурациялайтын Серверден ерекшеленеді.
  - **Жоқ**. Құрылғыларды жылжыту ережесі тек ағымдағы басқару сервері басқаратын клиенттік құрылғыларға қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

Бағдарламалар қойыншасы

Бұл қойыншада клиент құрылғыларында орнатылған басқарылатын бағдарламалар мен операциялық жүйелер негізінде құрылғыларды жылжыту ережесін конфигурациялауға болады:

- **Желілік агент орнатылған**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек Желілік агент орнатылған клиент құрылғыларына қолданылады.
  - **Жоқ**. Құрылғыларды жылжыту ережесі желілік агент орнатылмаған клиенттік құрылғыларға ғана қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **Бағдарламалар**

  Бұл құрылғыларға құрылғыларды жылжыту ережесі қолданылуы үшін клиент құрылғыларында қандай басқарылатын бағдарламалар орнатылуы керек екенін көрсетіңіз. Мысалы, **Kaspersky Security Center 15.1 Желілік агенті** немесе **Kaspersky Security Center 15.1 Басқару сервері** тармағын таңдаңыз.

  Егер сіз басқарылатын бағдарламаны таңдамасаңыз, шарт қолданылмайды.

- **Операциялық жүйенің нұсқасы**

  Операциялық жүйенің нұсқасына негізделген клиент құрылғыларын таңдауға болады. Ол үшін клиент құрылғыларында орнатылатын операциялық жүйелерді көрсетіңіз. Нәтижесінде, құрылғыларды жылжыту ережесі таңдалған операциялық жүйелері бар клиент құрылғыларына қолданылады.

  Бұл параметрі өшірулі болса, шарт қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Операциялық жүйенің биттік өлшемі**

  Сіз клиент құрылғыларын операциялық жүйенің бит өлшеміне қарай таңдай аласыз. **Операциялық жүйенің биттік өлшемі** өрісінде келесі мәндердің бірін таңдауға болады:

  - **Белгісіз**
  - **x86**
  - **AMD64**
  - **IA64**

  Клиент құрылғыларының операциялық жүйесінің архитектурасын тексеру үшін:

  1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
  2. Оң жақта **Бағандар параметрлері** түймесін (⚙) басыңыз.
  3. **Операциялық жүйенің биттік өлшемі** параметрін таңдап, **Сақтау** түймесін басыңыз.

     Осыдан кейін әрбір басқарылатын құрылғы үшін операциялық жүйенің архитектурасы көрсетіледі.

- **Операциялық жүйенің қызметтік бума нұсқасы**

  Бұл өрісте операциялық жүйенің пакет нұсқасын (*X.Y* форматында) көрсетуге болады, ол жылжыту ережесінің құрылғыға қалай қолданылатынын анықтайды. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **Пайдаланушы сертификаты**

  Келесі мәндердің бірін таңдаңыз:

  - **Орнатылған**. Құрылғыларды жылжыту ережесі тек ұялы құрылғы сертификаты бар ұялы құрылғыларға қолданылады.
  - **Орнатылмаған**. Құрылғыларды жылжыту ережесі тек ұялы құрылғы сертификаты жоқ ұялы құрылғыларға қатысты қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

- **Операциялық жүйе құрастырылымы**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілген нөмірден басқа барлық құрастыру нөмірлері үшін құрылғыларды жылжыту ережелерін конфигурациялауға болады.

- **Операциялық жүйе шығарылымының нөмірі**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш жинақ нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілген нөмірден басқа барлық жинақ нөмірлері үшін құрылғыларды жылжыту ережелерін конфигурациялауға болады.

Виртуалды машиналар қойыншасы

Бұл қойыншада, құрылғылардың виртуалды машиналар немесе виртуалды жұмыс үстелдері инфрақұрылымының (VDI) бөлігі екендігіне байланысты, бұл клиент құрылғыларын жылжыту ережелерінің параметрлерін конфигурациялауға болады:

- **Виртуалды машина болып табылады**

  Ашылмалы тізімде келесі мәндердің бірін таңдай аласыз:

  - **Қолданылмайды**. Шарт қолданылмайды.
  - **Жоқ**. Виртуалды машиналар емес құрылғыларды жылжыту.
  - **Иә**. Жылжытылатын құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

- **Virtual Desktop Infrastructure бөлігі**

  Ашылмалы тізімде келесі мәндердің бірін таңдай аласыз:

  - **Қолданылмайды**. Шарт қолданылмайды.
  - **Жоқ**. VDI бөлігі емес құрылғыларды жылжыту.
  - **Иә**. Жылжытылатын құрылғылар VDI бөлігі болуы керек.

Домен контроллері қойындысы

Бұл қойындыда доменнің ұйымдық бөлімшесінің құрамына кіретін құрылғыларды жылжыту қажет екенін көрсете аласыз. Сондай-ақ құрылғыларды көрсетілген домен бөлімшесінің барлық еншілес бөлімшелерінен жылжытуға болады:

- **Құрылғы келесі ұйымдық бөлімшеде қамтылған**

  Егер бұл параметр қосулы болса, құрылғыларды жылжыту ережесі параметрдегі тізімде көрсетілген доменнің ұйымдық бөлімшесіндегі құрылғыларға қолданылады.

  Әдепкі бойынша, параметр өшірулі.

- **Еншілес ұйымдық бөлімшелерін қосу**

  Бұл параметр қосулы болса, доменнің көрсетілген ұйымдық бірлігінің еншілес бөлімшелеріне кіретін құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғыларды еншілес бөлімшелерден сәйкес ішкі топтарға жылжыту**
- **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау**
- **Доменде жоқ қосалқы топтарды жою**
- **Құрылғы келесі доменнің қауіпсіздік тобында қамтылған**

  Егер бұл параметр қосылса, құрылғыларды жылжыту ережесі параметрдегі тізімде доменнің қауіпсіздік тобындағы құрылғыларға қатысты қолданылады.

  Әдепкі бойынша, параметр өшірулі.

Бұлттық сегменттер қойыншасы

Бұл қойындыда белгілі бір бұлттық сегменттерге жататын құрылғыларды жылжыту қажет екенін көрсетуге болады:

- **Құрылғы бұлттық сегментте орналасқан**

  Бұл параметрді таңдағанда, құрылғыларды жылжыту ережесі бұлттық сегментке жататын клиент құрылғыларына қатысты қолданылады. Параметрдің астындағы тізімдегі ішкі желіге дейін қажетті бұлттық сегментті таңдауға болады.

  Әдепкі бойынша, параметр өшірулі.

- **Қосалқы нысандарды қосу**

  Бұл параметрді таңдағанда, құрылғыларды жылжыту ережесі таңдалған бұлттық сегментке ғана емес, сонымен қатар осы сегменттің еншілес нысандарына да қолданылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғыларды кірістірілген нысандардан сәйкес қосалқы топтарға жылжыту**

- **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау**

- **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою**

- **Құрылғы API арқылы табылды**

  Ашылмалы тізімнен, құрылғының API құралдарымен анықталады ма екенін таңдауға болады:

  - **AWS**. Құрылғы AWS API арқылы табылды, яғни құрылғы AWS бұлтты ортасында орналасқан.
  - **Azure**. Құрылғы Azure API арқылы табылды, яғни құрылғы Azure бұлтты ортасында орналасқан.
  - **Google Cloud.** Құрылғы Google API арқылы табылды, яғни құрылғының Google Cloud ортасында орналасқаны анық.
  - **Жоқ**. Құрылғыны AWS, Azure немесе Google API пайдалану арқылы анықтау мүмкін емес, яғни ол бұлттық ортадан тыс немесе бұлттық ортада, бірақ оны API арқылы анықтау мүмкін емес.
  - **Көрсетілмеген**. Бұл шарт қолданылмайды.

Кластерлер мен серверлердің массивтері туралы

Kaspersky Security Center кластерлік технологияны қолдайды. Желілік агент Басқару серверіне клиент құрылғысында орнатылған бағдарлама сервер массивінің бөлігі екені туралы ақпарат берсе, онда клиент құрылғысы кластер түйініне айналады.

Басқару топта серверлердің кластерлері немесе массивтері болса, **Басқарылатын құрылғылар** бетінде екі қойынды көрсетіледі: біреуі жеке құрылғылар үшін, екіншісі серверлердің кластерлері мен массивтері үшін. Басқарылатын құрылғылар кластер түйіндері ретінде анықталғаннан кейін, кластер **Кластерлер және серверлердің массивтері** қойындысына бөлек нысан ретінде қосылады.

Кластер түйіндері немесе сервер массивтері басқа басқарылатын құрылғылармен бірге **Құрылғылар** қойындысында берілген. Түйіндердің сипаттарын жеке құрылғылар ретінде көруге және басқа операцияларды орындауға болады, бірақ кластер түйінін жою немесе оны кластерден бөлек басқа басқару тобына жылжыту мүмкін емес. Бүкіл кластерді ғана жоюға немесе жылжытуға болады.

Сервер кластерлерінде немесе массивтерінде келесі әрекеттерді орындауға болады:

- Сипаттарды көру.
- Кластерді немесе серверлер массивін басқа басқару топқа жылжыту.

  Кластерді немесе серверлер массивін басқа топқа жылжытқанда, оның барлық түйіндері онымен бірге жылжытылады, өйткені кластер және оның кез келген түйіні әрқашан бір басқару топқа жатады.

- Жою

  Серверлер кластері немесе массиві ұйымның желісінде бұдан былай болмаған кезде ғана серверлердің кластерін немесе массивін жойған дұрыс. Кластер әлі де желіңізде көрінсе және желілік агент пен Kaspersky қолданбасы кластер түйіндерінде әлі орнатылған болса, Kaspersky Security Center қашықтағы кластерді және оның түйіндерін басқарылатын құрылғылар тізіміне автоматты түрде қайтарады.

Кластерлердің немесе серверлердің массивтерінің сипаттары

Серверлер кластерінің немесе массивінің параметрлерін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** → **Кластерлер және серверлердің массивтері** бөліміне өтіңіз.

   Сервер кластерлері мен массивтерінің тізімі көрсетіледі.

2. Сервердің қажетті кластерінің немесе массивінің атын басыңыз.

Таңдалған сервер кластерінің немесе массивінің сипаттар терезесі ашылады.

Жалпы

Жалпы бөлімінде серверлердің кластері немесе массиві туралы жалпы ақпарат көрсетіледі. Ақпарат, кластер түйіндерін Басқару сервермен соңғы рет синхрондау барысында алынған деректер негізінде ұсынылады:

- **Атауы**
- **Сипаттама**
- **Windows домені**

  Сервердің кластерін немесе массивін қамтитын Windows домені немесе жұмыс тобы.

- **NetBIOS атауы**

  Windows желісіндегі серверлер кластерінің немесе массивінің атауы.

- **DNS атауы**

  Сервер кластерінің немесе массивінің DNS домен атауы.

Тапсырмалар

Тапсырмалар қойындысында сервер кластерлеріне және массивтеріне тағайындалған тапсырмаларды басқаруға болады: бар тапсырмалар тізімін қарау, жаңаларын жасау, жою, тапсырмаларды бастау және тоқтату, тапсырма параметрлерін өзгерту және орындау нәтижелерін қарау. Берілген тапсырмалар кластер түйіндеріне орнатылған Kaspersky қауіпсіздік қолданбасына қатысты. Kaspersky Security Center кластер түйіндерінен тапсырмалар тізімін және тапсырма күйі туралы ақпаратты алады. Байланыс болмаған жағдайда, күй көрсетілмейді.

Түйіндер

Бұл қойындыда серверлердің кластерінің немесе массивінің бөлігі болып табылатын түйіндер тізімі көрсетіледі. Құрылғы сипаттары терезесін көру үшін түйін атауын басуға болады.

Kaspersky қолданбасы

Сипаттар терезесінде кластер түйіндеріне орнатылған Kaspersky қауіпсіздік қолданбасына қатысты ақпарат пен параметрлері бар қосымша қойындылар да болуы мүмкін.

Құрылғы белсенді емес кезде әрекеттерді қарау және конфигурациялау

Егер басқару тобының клиент құрылғылары белсенді болмаса, сіз бұл туралы хабарландыру ала аласыз. Сондай-ақ, мұндай құрылғыларды автоматты түрде жоюға болады.

Басқару тобында құрылғылар белсенді болмаған кезде әрекеттерді көру немесе конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Қажетті басқару тобының атауын таңдаңыз.

   Басқару тобының сипаттары терезесі ашылады.
3. Сипаттар терезесінде **Параметрлер** қойыншасына өтіңіз.
4. **Иелену** бөлімінде келесі параметрлерді қосыңыз немесе өшіріңіз:

   - **Тектік топтан иелену**

     Егер жалауша қойылса, осы бөлімдегі параметрлер клиент құрылғысы кіретін тектік топтан иеленетін болады. Егер жалауша қойылса, **Құрылғының желідегі белсенділігі** параметрлер блогындағы параметрлерді өзгерту мүмкін емес.

     Бұл параметр тектік басқару тобы бар басқару тобы үшін ғана қолжетімді.

     Әдепкі бойынша, параметр қосулы.

   - **Еншілес топтардағы параметрлерді мәжбүрлеп иелену**

     Параметрлер мәндері еншілес топтарға бөлінеді, бірақ еншілес топтардың сипаттарында бұл параметрлер өзгертулер үшін қолжетімді емес.

     Әдепкі бойынша, параметр өшірулі.
5. **Құрылғы белсенділігі** бөлімінде келесі параметрлерді қосыңыз немесе өшіріңіз:

   - **Құрылғы мынанша (тәулік) астам белсенді емес болса, әкімшіге хабарлау**

     Егер бұл параметр қосулы болса, әкімші құрылғылардың белсенді еместігі туралы хабарландыру алады. Енгізу өрісінде сіз **Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды** оқиғасын қалыптастыратын уақыт аралығын орната аласыз. Әдепкі бойынша белгіленген уақыт аралығы – 7 күн.

     Әдепкі бойынша, параметр қосулы.

- **Мына уақыттан көбірек белсенді емес болса, құрылғыны топтан жойыңыз (тәулік)**

  Егер бұл параметр қосулы болса, құрылғы басқару тобынан автоматты түрде жойылатын уақыт аралығын көрсетуге болады. Әдепкі бойынша белгіленген уақыт аралығы – 60 күн.

  Әдепкі бойынша, параметр қосулы.

6. **Сақтау** түймесін басыңыз.

Сіздің өзгертулеріңіз сақталды және қолданылды.

Құрылғы күйлері туралы

Kaspersky Security Center бағдарламасы әрбір басқарылатын құрылғыға күй тағайындайды. Нақты күйі, пайдаланушы анықтаған шарттардың орындалғанына байланысты. Кейбір жағдайларда Kaspersky Security Center құрылғысына күй тағайындау кезінде құрылғының желіде көрінуін ескереді (төмендегі кестені қараңыз). Мысалы, басқарылатын құрылғыға *Критикалық* күйі берілген болса, *Дерекқорлар ескірген* шарты орындалғандықтан, құрылғы үшін көзге көрінетін болғандықтан, құрылғыға *ОК* күйі беріледі. Егер Kaspersky Security Center құрылғыны екі сағат ішінде желіден таппаса, құрылғының көрінуі *Офлайн* мәніне ие болады.

Келесі күйлер бар:

- *Критикалық* немесе *Критикалық / Көзге көрінетін*.
- *Ескерту* немесе *Ескерту / Көзге көрінетін*.
- *ОК* немесе *ОК / Көзге көрінетін*.

Төмендегі кестеде құрылғыға *Критикалық* немесе *Ескерту* күйін және олардың мүмкін мәндерін тағайындау үшін әдепкі бойынша шарттар келтірілген.

Құрылғыға күйлер белгілеу шарттары

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қауіпсіздік бағдарламасы орнатылмаған	Желілік агент құрылғыға орнатылған, бірақ қауіпсіздік бағдарламасы орнатылмаған.	• Қосқыш қосулы. • Қосқыш өшірулі.
Тым көп вирус анықталды	Вирустарды іздеу тапсырмаларының, мысалы, *Зиянды БҚ іздеу* тапсырмаларының жұмысы нәтижесінде, құрылғыда вирустар табылды және анықталған вирустардың саны көрсетілген мәннен асып түседі.	0-ден артық.
Нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше	Құрылғы желіде көрінеді, бірақ құрылғы күйіне арналған шартта нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше.	• Тоқтатылды. • Кідіртілді. • Орындалуда.
Зиянды бағдарлама сканерлеуі ұзақ уақыт орындалмады	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ *Зиянды БҚ іздеу* тапсырмасы да, жергілікті тексеру тапсырмасы да көрсетілген уақыттан артық орындалмады. Шарт тек жеті күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Дерекқорлар ескірген	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ антивирустық дерекқорлар бұл құрылғыда көрсетілген уақыттан артық жаңартылмаған. Шарт тек бір күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Қосылмағанына көп болды	Желілік агент құрылғыға орнатылған, бірақ құрылғы Басқару серверіне көрсетілген уақыттан артық қосылмаған, себебі құрылғы өшірулі.	1-күннен артық.
Белсенді қауіптер анықталды	**Белсенді қауіптер** қалтасындағы өңделмеген нысандар саны көрсетілген мәннен асып түседі.	0 данадан артық.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қайта іске қосу керек	Құрылғы желіде көрінеді, бірақ бағдарлама таңдалған себептердің біріне байланысты құрылғыны белгіленген уақыттан ұзағырақ қайта жүктеуді талап етеді.	0 минуттан көбірек.
Үйлесімді емес бағдарламалар орнатылды	Құрылғы желіде көрінеді, бірақ Желілік агент орындаған бағдарламалық жасақтаманы түгендеу кезінде, құрылғыда үйлесімсіз бағдарламалардың орнатылғаны анықталды.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарламалық жасақтама осалдықтары анықталды	Құрылғы желіде көрінеді және оған Желілік агент орнатылған, бірақ *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын орындау нәтижесінде құрылғыда критикалық деңгейі белгіленген бағдарламаларда осалдықтар анықталды.	• Критикалық. • Жоғары. • Орташа. • Осалдықты жабу мүмкін емес болса, елемеу. • Жаңарту орнатуға белгіленген болса, елемеу.
Лицензия мерзімі өтті	Құрылғы желіде көрінеді, бірақ лицензияның жарамдылық мерзімі өтіп кеткен.	• Қосқыш өшірулі. • Қосқыш қосулы.
Лицензияның қолданылу мерзімі жақында аяқталады	Құрылғы желіде көрінеді, бірақ лицензиялық жарамдылық мерзімі көрсетілген күндер санынан аз уақыттан кейін өтіп кетеді.	0 күннен аз.
Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады	Құрылғы желіде көрінеді, бірақ *Windows Update жаңартуларын синхрондау* тапсырмасы көрсетілген уақыт аралығында орындалмаған.	1-күннен артық.
Жарамсыз шифрлау күйі	Желілік агент құрылғыға орнатылған, бірақ құрылғыны шифрлау нәтижесі көрсетілген мәнге тең.	• Пайдаланушының бас тартуына байланысты саясатқа сәйкес келмейді (тек сыртқы құрылғылар үшін). • Қатеге байланысты саясатқа сай емес. • Саясат қолданылуда – қайта іске қосу қажет. • Шифрлау саясаты белгіленбеген. • Қолдау көрсетілмейді. • Саясат қолданылуда.
Ұялы құрылғы параметрлері саясатқа жауап бермейді	Ұялы құрылғының параметрлері сәйкестік ережелерін тексеру кезінде Kaspersky Endpoint Security for Android саясатында белгіленген параметрлерден ерекшеленеді.	• Қосқыш өшірулі. • Қосқыш қосулы.
Өңделмеген қауіпсіздік мәселелері табылды	Құрылғыда өңделмеген қауіпсіздік мәселелері бар. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарлама анықтаған құрылғы күйі	Құрылғының күйін басқарылатын бағдарлама анықтайды. Басқарылатын құрылғылар Kaspersky Security Center параметрлеріне қарамастан басқарылатын қолданбалармен анықталған күйге ие болуы мүмкін. Бұл күй Kaspersky Security Center анықтаған күйлердің бірін қайтарғаннан кейін, Басқару сервер басқарылатын құрылғыға басқарылатын құрылғы қайтарған және Басқару сервер тағайындағандардың ең маңызды күйін тағайындайды. Басқарылатын қолданбалар анықтаған күйлердің басқарылатын қолданбалар арқылы берілген сипаттамалары бар. Сипаттамаларды басқарылатын құрылғылар тізімінде, **Күйдің сипаттамасы** бағанында көре аласыз.	• Қосқыш өшірулі. • Қосқыш қосулы.
Құрылғыда бос орын жоқ	Құрылғының бос диск кеңістігі көрсетілген мәннен аз немесе құрылғы Басқару серверімен синхрондала алмайды. Құрылғы Басқару серверімен сәтті синхрондалғанда және құрылғының бос диск кеңістігі көрсетілген мәннен көп немесе тең болса, *Критикалық* немесе *Ескерту* күйлері *ОК* күйіне өзгереді.	0 МБ-тан көбірек.
Құрылғы басқарылмайтын күйге айналды	Құрылғылар табылған кезде құрылғы желіде көрінетін болып анықталады, бірақ Басқару серверімен синхрондаудың үштен артық сәтсіз әрекеті орындалды.	• Қосқыш өшірулі. • Қосқыш қосулы.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қорғаныс өшірілген	Құрылғы көзге көрінеді, бірақ құрылғыдағы қауіпсіздік бағдарламасы көрсетілген уақыттан артық өшірулі. Бұл жағдайда қауіпсіздік бағдарламасының күйі *Тоқтатылған* немесе *Ақау* болып табылады және келесілерден ерекшеленеді: *Іске қосылуда*, *Орындалуда*, немесе *Кідіртілді*.	0 минуттан көбірек.
Қауіпсіздік бағдарламасы іске қосылмаған	Құрылғы көзге көрінеді және қауіпсіздік бағдарламасы құрылғыда орнатылған, бірақ іске қосылмаған.	• Қосқыш өшірулі. • Қосқыш қосулы.

Kaspersky Security Center бағдарламасы белгіленген шарттарды орындау кезінде басқару тобындағы құрылғы күйін автоматты түрде ауыстырып қосуды конфигурациялауға мүмкіндік береді. Белгіленген шарттарды орындау кезінде, клиент құрылғысына келесі күйлердің бірі беріледі: *Критикалық* немесе *Ескерту*. Белгіленген шарттарды орындамаған жағдайда, клиент құрылғысына *ОК* күйі беріледі.

Бір шарттың әртүрлі мәндеріне әртүрлі күйлер сәйкес келуі мүмкін. Мысалы, әдепкі бойынша **3 күннен артық** мәні бар **Дерекқорлар ескірген** шартын ұстанған кезде клиент құрылғысына *Ескерту* күйі, ал **7 күннен артық** мәні бар шартты ұстанған кезде клиент құрылғысына *Критикалық* күйі беріледі.

Kaspersky Security Center бағдарламасын алдыңғы нұсқасынан жаңартып жатсаңыз, *Критикалық* немесе *Ескерту* күйін тағайындау үшін **Дерекқорлар ескірген** шартының мәні өзгермейді.

Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Ашылған топтар тізімінде құрылғылардың күйлерін ауыстырып қосуды өзгерткіңіз келетін топтың атауы бар сілтемеден өтіңіз.
3. Пайда болған сипаттар терезесінде **Құрылғының күйі** қойыншасын таңдаңыз.
4. **Критикалық** бөлімін таңдаңыз.
5. **Егер олар көрсетілген болса, Критикалыққа орнатыңыз** блогында құрылғыны *Критикалық* күйіне ауыстырып қосу үшін шартты қосыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.

9. **ОК** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Ашылған топтар тізімінде құрылғылардың күйлерін ауыстырып қосуды өзгерткіңіз келетін топтың атауы бар сілтемеден өтіңіз.
3. Пайда болған сипаттар терезесінде **Құрылғының күйі** қойыншасын таңдаңыз.
4. **Ескерту** бөлімін таңдаңыз.
5. **Егер олар көрсетілген болса, Ескертуге орнатыңыз** блогында құрылғыны *Ескерту* күйіне ауыстырып қосу үшін шартты қосыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.

9. **OK** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Ескерту* күйі тағайындалады.

Клиент құрылғысының жұмыс үстеліне қашықтан қосылу

Әкімші құрылғыда орнатылған Желілік агент арқылы клиент құрылғысының жұмыс үстеліне қашықтан қатынаса алады. Желілік агентті пайдаланып клиент құрылғысына қашықтан қосылу, клиент құрылғысының TCP және UDP порттары қатынасу үшін жабық болған жағдайда да мүмкін болады.

Құрылғыға қосылғаннан кейін, әкімші осы құрылғыдағы ақпаратқа толық қатынас алады және онда орнатылған бағдарламаларды басқара алады.

Қашықтан қосылу, мақсатты басқарылатын құрылғының операциялық жүйесінің параметрлерінде рұқсат етілуі тиіс. Мысалы, Windows 10 жүйесінде бұл параметр **Қашықтағы көмекшіні осы компьютерге қосуға рұқсат беру** деп аталады (оны **Басқару тақтасы** → **Жүйе және қауіпсіздік** → **Жүйе** → **Қашықтан қатынасуды конфигурациялау** тармағынан табуға болады). Осалдықтар мен патчтарды басқаруға лицензияңыз болса, басқарылатын құрылғымен қосылым орнатылған кезде осы параметрді мәжбүрлеп қоса аласыз. Лицензияңыз болмаса, осы параметрді мақсатты басқарылатын құрылғыда жергілікті түрде қосыңыз. Осы параметр өшірулі болса, қашықтан қосылу мүмкін емес.

Құрылғымен қашықтан қосылым орнату үшін сізде екі утилита болуы тиіс:

- Kaspersky klsctunnel утилитасы. Бұл утилита әкімшінің жұмыс станциясында сақталуы тиіс. Сіз осы утилитаны, клиент құрылғысы мен Басқару сервері арасында байланысты туннельдеу үшін қолданасыз.

Kaspersky Security Center бағдарламасы Басқару консолінен TCP қосылымдарын Басқару сервері арқылы және одан әрі Желілік агент арқылы басқарылатын құрылғыдағы белгіленген портқа туннельдеуге мүмкіндік береді. Туннельдеу, егер Басқару консолі бар құрылғыны құрылғыға тікелей қосу мүмкін болмаса, Басқару консолі орнатылған құрылғыдағы клиент қолданбасын басқарылатын құрылғыдағы TCP портына қосу үшін қолданылады.

Қашықтағы клиент құрылғысы мен Басқару сервері арасындағы байланысты туннельдеу, құрылғыда Басқару серверіне қосылуға арналған порт қолжетімді болмаған кезде қажет. Құрылғыдағы порт келесі жағдайларда қолжетімді болмауы мүмкін:

- Қашықтағы құрылғы NAT механизмі қолданылатын жергілікті желіге қосылған.
- Қашықтағы құрылғы Басқару серверінің жергілікті желісіне кіреді, бірақ оның порты желілік экранмен жабылған.

- Microsoft Windows "Қашықтағы жұмыс үстеліне қосылу орындалуда" стандартты құрамдасы. Қашықтағы жұмыс үстеліне қосылу Windows mstsc.exe штаттық утилитасы арқылы, осы утилитаның жұмыс параметрлеріне сай орындалады.

  Пайдаланушының қашықтағы жұмыс үстелінің қолданыстағы сеансына қосылу, пайдаланушыны хабарландырусыз жүзеге асырылады. Әкімшіні сеансқа қосқаннан кейін, құрылғының пайдаланушысы сеанстан алдын ала хабарландырусыз өшіріледі.

Клиент құрылғысының жұмыс үстеліне қашықтан қосылу үшін:

1. MMC негізіндегі Басқару консолінде, Басқару сервері саясатының контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
2. Ашылған Басқару сервері сипаттары терезесінде **Басқару серверіне қосылу параметрлері → Қосылу порттары** бөліміне өтіңіз.
3. **Kaspersky Security Center Web Console үшін RDP портын ашу** параметрі қосулы екеніне көз жеткізіңіз.
4. Kaspersky Security Center Web Console серверінде **Активтер (құрылғылар) → Басқарылатын құрылғылар** бөліміне өтіңіз.
5. Басқарылатын құрылғылар тізімінің үстіндегі **Ағымдағы жол** өрісінде сілтеме бойынша өтіңіз.
6. Сол жақта ашылған панельде қол жеткізгіңіз келетін құрылғыны қамтитын басқару тобын таңдаңыз.
7. Қатынас алғыңыз келетін құрылғыға қарама-қарсы жалауша қойыңыз.
8. **Қашықтағы жұмыс үстеліне қосылу** түймесін басыңыз.

   Қашықтағы жұмыс үстелі (тек Windows) терезесі ашылады.
9. **Басқарылатын құрылғыда қашықтағы жұмыс үстеліне қосылуға рұқсат ету** параметрін қосыңыз. Бұл жағдайда, қашықтан қосылуға қазіргі уақытта басқарылатын құрылғыдағы операциялық жүйенің параметрлерінде тыйым салынған болса да, байланыс орнатылады.

   Бұл параметр тек Осалдықтар мен патчтарды басқару лицензиясы болған жағдайда ғана қолжетімді.
10. klsctunnel утилитасын жүктеу үшін **Жүктеп алу** түймесін басыңыз.

11. Мәтіндік өрістен мәтінді көшіріп алу үшін **Аралық сақтағышқа көшіру** түймесін басыңыз. Бұл мәтін, Басқару сервері мен басқарылатын құрылғы арасында байланыс орнатуға қажетті параметрлерді қамтитын екілік деректер нысаны (BLOB) болып табылады.

    BLOB нысаны 3 минут бойы жарамды. Оның мерзімі өтіп кетсе, жаңа үлкен екілік нысан жасау үшін Қашықтағы жұмыс үстелі (тек Windows) терезесін қайта ашыңыз.

12. klsctunnel утилитасын іске қосыңыз.

    Утилита терезесі ашылады.

13. Көшіріп алынған мәтінді мәтіндік өріске салыңыз.

14. Прокси-серверді қолдансаңыз, **Прокси-серверді пайдалану** жалаушасын орнатыңыз, содан соң прокси-серверге қосылу параметрлерін көрсетіңіз.

15. **Портты ашу** түймесін басыңыз.

    Қашықтағы жұмыс үстеліне қосылу жүйесіне кіру терезесі ашылады.

16. Kaspersky Security Center Web Console веб-консоліне қазір кіріп жатқан есептік жазбаның есептік деректерін көрсетіңіз.

17. **Қосылу** түймесін басыңыз.

Клиент құрылғысына қосылғаннан кейін, клиент құрылғысының жұмыс үстелі Microsoft Windows қашықтан қосылу терезесінде қолжетімді.

Windows компьютерлік бөлісу қызметі арқылы құрылғыларға қосылу

Әкімші құрылғыда орнатылған Желілік агент арқылы клиент құрылғысының жұмыс үстеліне қашықтан қатынаса алады. Желілік агентті пайдаланып клиент құрылғысына қашықтан қосылу, клиент құрылғысының TCP және UDP порттары қатынасу үшін жабық болған жағдайда да мүмкін болады.

Әкімші клиент құрылғысында қолданылатын сеансқа, сол сеанста жұмыс істейтін пайдаланушыны ажыратпай, қосыла алады. Бұл жағдайда, құрылғыдағы әкімші мен сеанс пайдаланушысы жұмыс үстеліне ортақ қол жеткізе алады.

Құрылғымен қашықтан қосылым орнату үшін сізде екі утилита болуы тиіс:

- Kaspersky klsctunnel утилитасы. Бұл утилита әкімшінің жұмыс станциясында сақталуы тиіс. Сіз осы утилитаны, клиент құрылғысы мен Басқару сервері арасында байланысты туннельдеу үшін қолданасыз.

  Kaspersky Security Center бағдарламасы Басқару консолінен TCP қосылымдарын Басқару сервері арқылы және одан әрі Желілік агент арқылы басқарылатын құрылғыдағы белгіленген портқа туннельдеуге мүмкіндік береді. Туннельдеу, егер Басқару консолі бар құрылғыны құрылғыға тікелей қосу мүмкін болмаса, Басқару консолі орнатылған құрылғыдағы клиент қолданбасын басқарылатын құрылғыдағы TCP портына қосу үшін қолданылады.

Қашықтағы клиент құрылғысы мен Басқару сервері арасындағы байланысты туннельдеу, құрылғыда Басқару серверіне қосылуға арналған порт қолжетімді болмаған кезде қажет. Құрылғыдағы порт келесі жағдайларда қолжетімді болмауы мүмкін:

- Қашықтағы құрылғы NAT механизмі қолданылатын жергілікті желіге қосылған.
- Қашықтағы құрылғы Басқару серверінің жергілікті желісіне кіреді, бірақ оның порты желілік экранмен жабылған.

- Windows жұмыс үстелін бірлесіп пайдалану. Қолданыстағы қашықтағы жұмыс үстелі сеансына қосылған кезде, құрылғыдағы осы сеанстың пайдаланушысы әкімшіден қосылуға сұрау алады. Құрылғымен қашықтан жұмыс істеу процесі және осы жұмыстың нәтижелері туралы ақпарат Kaspersky Security Center есептерінде сақталмайды.

  Әкімші қашықтағы клиент құрылғысында әрекеттер аудитін конфигурациялай алады. Аудит барысында, бағдарлама әкімші ашқан және/немесе өзгерткен клиент құрылғысындағы файлдар туралы ақпаратты сақтайды.

Windows жұмыс үстелін бірлесіп пайдалану арқылы клиент құрылғысының жұмыс үстеліне қосылу үшін келесі шарттар орындалуы керек:

- Әкімшінің жұмыс станциясында Microsoft Windows Vista операциялық жүйесі немесе одан кейінгі нұсқасы орнатылған. Басқару сервері орнатылған құрылғының операциялық жүйесінің түрі Windows компьютерлік бөлісу қызметі арқылы қосылуға шектеу емес.

  Windows нұсқаңызда Windows Жұмыс үстелін бірлесіп пайдалану функциясы қосылғанын тексеру үшін Windows тізімдемесінде CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} қосулы екеніне көз жеткізіңіз.

- Клиент құрылғысында Microsoft Windows Vista операциялық жүйесі немесе одан кейінгі нұсқасы орнатылған.

- Kaspersky Security Center бағдарламасы Осалдықтар мен патчтарды басқаруға арналған лицензияны қолданады.

Windows жұмыс үстелін бірлесіп пайдалану арқылы клиент құрылғысының Windows жұмыс үстеліне қосылу үшін:

1. MMC негізіндегі Басқару консолінде, Басқару сервері саясатының контекстік мәзірінен **Сипаттар** тармағын таңдаңыз.
2. Ашылған Басқару сервері сипаттары терезесінде **Басқару серверіне қосылу параметрлері → Қосылу порттары** бөліміне өтіңіз.
3. **Kaspersky Security Center Web Console үшін RDP портын ашу** параметрі қосулы екеніне көз жеткізіңіз.
4. Kaspersky Security Center Web Console серверінде **Активтер (құрылғылар) → Басқарылатын құрылғылар** бөліміне өтіңіз.
5. Басқарылатын құрылғылар тізімінің үстіндегі **Ағымдағы жол** өрісінде сілтеме бойынша өтіңіз.
6. Сол жақта ашылған панельде қол жеткізгіңіз келетін құрылғыны қамтитын басқару тобын таңдаңыз.
7. Қатынас алғыңыз келетін құрылғыға қарама-қарсы жалауша қойыңыз.
8. **Windows компьютерлік бөлісу қызметін пайдалану** түймесін басыңыз.

   Windows компьютерлік бөлісу қызметін пайдалану шебері ашылады.

9. klsctunnel утилитасын жүктеп алу үшін **Жүктеп алу** түймесін басыңыз және жүктеп алу процесінің аяқталуын күтіңіз.

   Сізде klsctunnel утилитасы бұрыннан бар болса, бұл қадамды өткізіп жіберіңіз.

10. **Келесі** түймесін басыңыз.

11. Қосылғыңыз келетін құрылғыдағы сеансты таңдап, **Келесі** түймесін басыңыз.

12. Ашылған терезеде мақсатты құрылғыда пайдаланушы жұмыс үстеліне ортақ қатынасу сеансына рұқсат беруі керек. Әйтпесе, сеансты бастау мүмкін емес.

    Құрылғы пайдаланушысы жұмыс үстелін ортақ пайдалану сеансын растағаннан кейін, шебердің келесі беті ашылады.

13. Мәтіндік өрістен мәтінді көшіріп алу үшін **Аралық сақтағышқа көшіру** түймесін басыңыз. Бұл мәтін, Басқару сервері мен басқарылатын құрылғы арасында байланыс орнатуға қажетті параметрлерді қамтитын екілік деректер нысаны (BLOB) болып табылады.

    > BLOB нысаны 3 минут бойы жарамды. Егер оның әрекет ету мерзімі өтіп кетсе, BLOB нысанын жасаңыз.

14. klsctunnel утилитасын іске қосыңыз.

    Утилита терезесі ашылады.

15. Көшіріп алынған мәтінді мәтіндік өріске салыңыз.

16. Прокси-серверді қолдансаңыз, **Прокси-серверді пайдалану** жалаушасын орнатыңыз, содан соң прокси-серверге қосылу параметрлерін көрсетіңіз.

17. **Портты ашу** түймесін басыңыз.

Жұмыс үстеліне ортақ қатынасу жаңа терезеде іске қосылады. Құрылғымен өзара әрекеттескіңіз келсе, терезенің жоғарғы сол жақ бұрышындағы мәзір () белгішесін басып, **Интерактивті режим** тармағын таңдаңыз.

Құрылғыны таңдаулары

Құрылғыны таңдалары – бұл белгіленген шарттарға сәйкес құрылғыларды сүзгілеуге арналған құрал. Бірнеше құрылғыны басқару үшін құрылғы таңдауларын пайдалануға болады: мысалы, тек таңдалған құрылғылар туралы есептерді көру немесе осы құрылғылардың барлығын басқа басқару тобына жылжыту.

Kaspersky Security Center бағдарламасы *құрылғының алдын ала анықталған таңдауларының* кең ауқымын ұсынады (мысалы, **Критикалық күйі бар құрылғылар**, **Қорғаныс өшірілген**, **Белсенді қауіптер анықталды**). Алдын ала анықталған таңдауды жоюға болмайды. Сондай-ақ қосымша *пайдаланушы анықтайтын таңдауларды* жасауға және конфигурациялауға болады.

Пайдаланушының таңдауларында іздеу аймағын белгілеуге және барлық құрылғыларды, басқарылатын құрылғыларды немесе тағайындалмаған құрылғыларды таңдауға болады. Іздеу параметрлері шарттарда белгіленеді. Құрылғы таңдауларында әртүрлі іздеу параметрлері бар бірнеше шарттар жасауға болады. Мысалы, сіз екі шарт жасай аласыз және әрқайсысында әртүрлі IP ауқымдарын белгілей аласыз. Егер бірнеше шарттар белгіленген болса, құрылғы таңдауларына кез келген шартты қанағаттандыратын құрылғылар енеді. Керісінше, бір шартта іздеу параметрлері бір-біріне қабаттасады. Егер таңдау шартында IP ауқымы және орнатылған бағдарламаның атауы белгіленген болса, онда құрылғы таңдауларына бір уақытта көрсетілген бағдарлама орнатылған және олардың IP мекенжайлары көрсетілген ауқымға кіретін құрылғылар ғана кіреді.

Құрылғы таңдауларынан құрылғылар тізімін қарау

Kaspersky Security Center құрылғы таңдауынан құрылғылар тізімін көруге мүмкіндік береді.

Құрылғы таңдауынан құрылғылар тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Құрылғы таңдаулары** немесе **Табу және орналастыру** → **Құрылғы таңдаулары** бөліміне өтіңіз.
2. Таңдаулар тізімінде құрылғыны таңдаудың атауын басыңыз.

   Бетте құрылғы таңдауына енгізілген құрылғылар туралы ақпараты бар кесте көрсетілген.
3. Құрылғылар кестесінің деректерін келесідей топтастыруға және сүзуге болады:
   - Параметрлер белгішесін (⚙) басыңыз және кестеде көрсетілетін бағандарды таңдаңыз.
   - (▽) сүзу белгішесін нұқыңыз, ашылған мәзірде сүзу критерийін көрсетіңіз және қолданыңыз.

     Сүзілген құрылғылар кестесі көрсетіледі.

Құрылғы таңдауында бір немесе бірнеше құрылғыны таңдап, осы құрылғыларға қолданылатын тапсырманы жасау үшін **Жаңа тапсырма**.

Таңдалған құрылғыларды құрылғы таңдауынан басқа басқару тобына жылжыту үшін **Топқа жылжыту** түймесін басыңыз және мақсатты басқару тобын таңдаңыз.

Құрылғы таңдауларын жасау

Құрылғы таңдауларын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Құрылғы таңдаулары** бөліміне өтіңіз.

   Құрылғылар таңдауы тізімі бар бет көрсетіледі.
2. **Қосу** түймесін басыңыз.

   Құрылғыны таңдау параметрлері терезесі ашылады.
3. Жаңа таңдау атауын енгізіңіз.
4. Құрылғы таңдауларына қосылатын құрылғыларды қамтитын топты көрсетіңіз:
   - **Кез келген құрылғыларды іздеу** – **Басқарылатын құрылғылар** немесе **Тағайындалмаған құрылғылар** топтарында таңдау шарттарына сәйкес келетін құрылғыларды іздеу.
   - **Басқарылатын құрылғыларды іздеу** – **Басқарылатын құрылғылар** тобында таңдау шарттарына сәйкес келетін құрылғыларды іздеу.
   - **Тағайындалмаған құрылғыларды іздеу** – **Тағайындалмаған құрылғылар** тобында таңдау шарттарына сәйкес келетін құрылғыларды іздеу.

   Қосалқы Басқару серверлерінде таңдау критерийлеріне сәйкес келетін құрылғыларды іздеуді қосу үшін **Қосалқы Басқару серверлерінен алынған деректерді қамту** жалаушасын қоя аласыз.

5. **Қосу** түймесін басыңыз.

6. Ашылған терезеде, құрылғыларды осы таңдауға қосу үшін орындалуы тиісті шарттарды көрсетіңіз және **OK** түймесін басыңыз.

7. **Сақтау** түймесін басыңыз.

Құрылғы таңдаулары жасалып, құрылғы таңдаулары тізіміне қосылған.

Құрылғы таңдауларын конфигурациялау

Құрылғы таңдаулары параметрлерін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Құрылғы таңдаулары** бөліміне өтіңіз.

   Құрылғылар таңдауы тізімі бар бет көрсетіледі.

2. Тиісті пайдаланушы құрылғылар таңдауын таңдап, **Сипаттар** түймесін басыңыз.

   Құрылғыны таңдау параметрлері терезесі ашылады.

3. **Жалпы** қойыншасында **Жаңа шарт** сілтемесінен өтіңіз.

4. Құрылғы осы таңдауға қосылуы үшін орындалуы керек шарттарды көрсетіңіз.

5. **Сақтау** түймесін басыңыз.

Параметрлер қолданылған және сақталған.

Төменде құрылғыларды таңдауға жатқызу шарттарының параметрлері сипатталған. Шарттар логикалық "немесе" бойынша біріктіріледі: ұсынылған шарттардың кем дегенде біреуін қанағаттандыратын құрылғылар таңдауға түседі.

Жалпы

Жалпы бөлімінде таңдау шартының атауын өзгертуге және осы шартты кері қайтару қажет пе екенін көрсетуге болады:

Таңдау шартын кері қайтару

Әдепкі бойынша, параметр өшірулі.

Бұл опцияны қоссаңыз, берілген таңдау шарты инверсияланады. Шартқа сәйкес келмейтін барлық құрылғылар таңдауға кіреді.

Келесі мысалда инверсия жұмысының логикасы көрсетілген:

- **Шарт**: құрылғыда Linux түріндегі операциялық жүйе және 00.0.000 құрастыру нөмірі бар.
- **Инверсияланған жағдай**: құрылғыда келесінің баламасы болатын NOT (Linux түрі және 00.0.000 құрастыру нөмірі) бар операциялық жүйе бар.

  NOT түріндегі Linux НЕМЕСЕ NOT 00.0.000 құрастыру нөмірі бар операциялық жүйе бар.

Осылайша таңдауға, мысалы, Windows түріндегі және 00.0.000 құрастыру нөмірі бар немесе Linux түріндегі және 00.0.000-ден басқа жинақ нөмірі бар құрылғылар кіреді.

Желі инфрақұрылымы

Желі бөлімінде құрылғыларды олардың желілік деректері негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғы атауы**

  Windows желісіндегі құрылғы атауы (NetBIOS атауы) немесе IPv4 мекенжайы не IPv6 мекенжайы.

- **Домен**

  Көрсетілген Windows доменіне кіретін барлық құрылғылар көрсетіледі.

- **Басқару тобы**

  Көрсетілген басқару тобына кіретін құрылғылар көрсетіледі.

- **Сипаттама**

  Құрылғы сипаттары терезесінде қамтылған мәтін: **Жалпы** бөлімінің **Сипаттама** өрісінде.

  Сипаттама мәтінінде келесі таңбаларды қолдануға болады:

  - Бір сөздің ішінде:

    - *****. 0 немесе одан да көп таңбадан ұзын кез келген жолды алмастырады.

    Мысалы:

    Сервер, **Серверлік** сөздерін сипаттау үшін **Сервер*** жолын қолдануға болады.

    - **?.** Кез келген бір таңбаны ауыстырады.

    Мысалы:

    Құралдар немесе **Құралдан** сөздерін сипаттау үшін **Құралда?** жолын қолдануға болады.

    Жұлдызша (*****) немесе сұрақ белгісі (**?**) мәтін сипаттамасында бірінші таңба ретінде қолданылуы мүмкін емес.

  - Бірнеше сөздерді байланыстыру үшін:

    - Бос орын. Сипаттамаларында аталған сөздердің кез келгені бар барлық құрылғыларды көрсетеді.

    Мысалы:

    Қосалқы немесе **Виртуалдық** сөзін қамтитын сөйлемшені сипаттау үшін **Қосалқы Виртуалды** жолын қолдануға болады.

    - **+**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болуын білдіреді.

    Мысалы:

    Қосалқы сөзін де, **Виртуалды** сөзін де қамтитын сөйлемшені сипаттау үшін **+Қосалқы+Виртуалды** жолын қолдануға болады.

    - **-**. Сөздің алдында жазған кезде, мәтінде сөздің міндетті түрде болмауын білдіреді.

    Мысалы:

Қосалқы сөзі болуы, бірақ **Виртуалды** сөзі болмауы тиісті сөйлемшені сипаттау үшін **+Қосалқы-Виртуалды** жолын қолдануға болады.

- **"<мәтін үзіндісі>"**. Тырнақшаға алынған мәтін үзіндісі мәтінде толығымен болуы керек.

Мысалы:

Қосалқы Сервер сөзтіркесін қамтитын сөйлемшені сипаттау үшін, **"Қосалқы Сервер"** жолын қолдануға болады.

- **IP ауқымы**

  Бұл параметр қосулы болса, енгізу өрістерінде сіз іздеген құрылғылар кіруі тиісті аралықтың бастапқы және соңғы IP мекенжайларын көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Басқа Басқару серверімен басқарылады**

  Келесі мәндердің бірін таңдаңыз:

  - **Иә**. Құрылғыларды жылжыту ережесі тек басқа Басқару серверлері басқаратын клиент құрылғыларына қолданылады. Бұл Серверлер құрылғыларды жылжыту ережесін конфигурациялайтын Серверден ерекшеленеді.
  - **Жоқ**. Құрылғыларды жылжыту ережесі тек ағымдағы басқару сервері басқаратын клиенттік құрылғыларға қолданылады.
  - **Мән таңдалмаған**. Шарт қолданылмайды.

Домен контроллері бөлімінде құрылғыларды домен мүшелігін таңдауға қосу өлшемшарттарын орнатуға болады:

- **Доменнің ұйымдық бөлімшесіндегі құрылғы**

  Егер бұл параметр қосулы болса, енгізу өрісінде көрсетілген домен бөлімшесіндегі құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы доменнің қауіпсіздік тобының мүшесі болып табылады**

  Егер бұл параметр қосулы болса, енгізу өрісінде көрсетілген доменнің қауіпсіздік тобындағы құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

Желілік белсенділік бөлімінде құрылғыларды олардың желілік белсенділігі негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Тарату нүктесі ретінде әрекет етеді**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға тарату нүктелері болып табылатын құрылғылар қосылады.
  - **Жоқ**. Тарату нүктелері ретінде әрекет ететін құрылғылар таңдауға кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверімен байланысты үзбеу**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Қосулы**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы қойылған құрылғыларды қамтиды.
  - **Өшірулі**. Таңдау **Басқару серверімен байланысты үзбеу** жалаушасы алынған құрылғыларды қамтиды.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қосылым профилі ауыстырылды**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Таңдауға қосылым профилін ауыстырып қосу нәтижесінде Басқару серверіне қосылған құрылғылар кіреді.
  - **Жоқ**. Таңдауға қосылым профилін ауыстыру нәтижесінде басқару серверіне қосылған құрылғылар кірмейді.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Басқару серверіне соңғы қосылу уақыты**

  Осы жалаушаны пайдаланып, Басқару серверіне соңғы қосылу уақыты бойынша құрылғыларды іздеу өлшемшартын белгілей аласыз.

  Егер жалауша қойылса, енгізу өрістерінде, клиент құрылғысында орнатылған Желілік агенттің Басқару серверіне соңғы қосылуы орындалған аралықтың мәндерін (күні мен уақыты) көрсетуге болады. Таңдауға белгіленген аралыққа сәйкес келетін құрылғылар қосылады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Жаңа құрылғылар желі сауалнамасымен анықталды**

  Соңғы бірнеше күнде желіде сауалнама өткізу кезінде табылған жаңа құрылғыларды іздеу.

  Егер бұл параметр қосулы болса, онда **Анықтау кезеңі (тәу)** өрісінде көрсетілген күндер санында құрылғыларды анықтау процесінде табылған жаңа құрылғылар ғана таңдауға қосылады.

  Егер бұл параметр өшірулі болса, онда құрылғыны анықтау процесінде табылған барлық құрылғылар таңдауға қосылады.

  Әдепкі бойынша, параметр өшірулі.

- **Құрылғы көрінеді**

  Ашылмалы тізімде, іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады:

  - **Иә**. Бағдарлама қазіргі уақытта желіде көрінетін құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қазіргі уақытта желіде көрінбейтін құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Бұлттық сегменттер бөлімінде, бұлттық сегменттерге сәйкес құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғы бұлттық сегментте орналасқан**

  Бұл параметр қосылса, AWS, Azure және Google бұлт сегменттерінен құрылғыларды таңдауға болады.

Қосалқы нысандарды қосу параметрі де қосулы болса, іздеу көрсетілген сегменттің барлық салынған нысандары бойынша жүргізіледі.

Іздеу нәтижелеріне тек таңдалған сегменттегі құрылғылар кіреді.

- **Құрылғы API арқылы табылды**

  Ашылмалы тізімнен, құрылғының API құралдарымен анықталады ма екенін таңдауға болады:

  - **Иә**. Құрылғы AWS, Azure немесе Google API арқылы анықталады.
  - **Жоқ**. Құрылғыны AWS, Azure немесе Google API арқылы анықтау мүмкін. Яғни, құрылғы бұлттық ортадан тыс немесе бұлттық ортада, бірақ қандай да бір себептермен API арқылы іздеу үшін қолжетімді емес.
  - Көрсетілмеген. Бұл шарт қолданылмайды.

Құрылғы күйлері

Басқарылатын құрылғы күйі бөлімінде, басқарылатын бағдарламадан құрылғы күйінің сипаттамасы бойынша таңдауға құрылғыларды қосу өлшемшарттарын конфигурациялауға болады:

- **Құрылғының күйі**

  Құрылғы күйлерінің бірін таңдауға болатын ашылмалы тізім: *OK*, *Критикалық* немесе *Ескерту*.

- **Нақты уақыт режимінде қорғау күйі**

  Нақты уақыт режимінде қорғау тапсырмасы күйінің мәнін таңдауға болатын ашылмалы тізім. Нақты уақыт режимінде қорғау күйі көрсетілген құрылғылар таңдауға қосылады.

- **Құрылғы күйінің сипаттамасы**

  Бұл өрісте орындалса, құрылғыға келесі күйлердің бірін тағайындайтын шарттардың жанындағы құсбелгі ұяшықтарын таңдай аласыз: *OK, Критикалық* немесе *Ескерту*.

Басқарылатын бағдарламалардың құрамдастарының күйі бөлімінде, басқарылатын бағдарламалардың құрамдастарының күйлері бойынша құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Деректердің жайылып кетуіне жол бермеу күйі**

  Деректердің жайылып кетуінен қорғау құрамдасының күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Бірлескен жұмыс серверлерінің қорғаныс күйі**

  Бірлескен жұмыс серверлері үшін қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз*, *Тоқтатылды*, *Іске қосылды, Кідіртілді*, *Орындалуда*, *Сәтсіз аяқталды*).

- **Пошталық серверлердің антивирустық қорғаныс күйі**

  Пошта серверінің қорғау күйі бойынша құрылғыларды іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

- **Endpoint Sensor күйі**

  Құрылғыларды Endpoint Sensor құрамдасының күйі бойынша іздеу (*Белгісіз, Тоқтатылды, Іске қосылды, Кідіртілді, Орындалуда, Сәтсіз аяқталды*).

Басқарылатын бағдарламалардағы күйге әсер ететін мәселелер бөлімінде, басқарылатын бағдарлама анықтаған ықтимал мәселелер тізіміне сәйкес құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады. Егер сіз таңдаған құрылғыда кем дегенде бір мәселе болса, құрылғы таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген мәселені таңдағанда, сізде барлық тізімдерде осы мәселені автоматты түрде таңдау мүмкіндігі болады.

Сіз басқарылатын бағдарламалар күйлерінің сипаттамасы үшін жалаушаларды қоя аласыз, оларды алған кезде құрылғылар таңдауға қосылады. Бірнеше бағдарлама үшін көрсетілген күйді таңдағанда, сізде барлық тізімдерде осы күйді автоматты түрде таңдау мүмкіндігі болады.

Жүйе мәліметтері

Операциялық жүйе бөлімінде, орнатылған операциялық жүйенің негізінде құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады.

- **Платформа түрі**

  Егер жалауша қойылса, тізімнен операциялық жүйелерді таңдауға болады. Көрсетілген операциялық жүйелер орнатылған құрылғылар іздеу нәтижелеріне қосылады.

- **Операциялық жүйенің қызметтік бума нұсқасы**

  Бұл өрісте операциялық жүйенің пакет нұсқасын (*X.Y* форматында) көрсетуге болады, ол жылжыту ережесінің құрылғыға қалай қолданылатынын анықтайды. Әдепкі бойынша, нұсқаның мәндері белгіленбеген.

- **Операциялық жүйенің биттік өлшемі**

  Ашылмалы тізімде операциялық жүйенің биттік өлшемін таңдауға болады, оның болуы бойынша құрылғыға құрылғыны жылжыту ережесі қолданылады (**Белгісіз**, **x86**, **AMD64** немесе **IA64**). Әдепкі бойынша, тізімде бірде-бір нұсқа таңдалмаған, операциялық жүйенің биттік өлшемі белгіленбеген.

- **Операциялық жүйе құрастырылымы**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйенің құрастыру нөмірі. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш құрастыру нөмірі болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық құрастыру нөмірлерін іздеуді конфигурациялауға болады.

- **Операциялық жүйе шығарылымының нөмірі**

  > Бұл параметр тек Windows операциялық жүйелері үшін қолданылады.

  Операциялық жүйе шығарылымының идентификаторы. Таңдалған операциялық жүйеде тең, анағұрлым ерте немесе анағұрлым кеш шығарылым идентификаторы болуы керек пе екенін көрсетуге болады. Сондай-ақ, көрсетілгеннен басқа барлық шығарылым идентификаторы нөмірлерін іздеуді конфигурациялауға болады.

Виртуалды машиналар бөлімінде, бұл құрылғылардың виртуалды машиналар немесе Virtual Desktop Infrastructure бөлігі екендігіне байланысты құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Виртуалды машина болып табылады**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Анықталмаған**.
  - **Жоқ**. Виртуалды машиналар емес құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар виртуалды машиналар болуы керек.

- **Виртуалды машинаның түрі**

  Ашылмалы тізімнен виртуалды машина өндірушісін таңдауға болады.

  Бұл ашылмалы тізім **Виртуалды машина болып табылады** ашылмалы тізімінде **Иә** немесе **Маңызды емес** мәні таңдалған болса қолжетімді.

- **Virtual Desktop Infrastructure бөлігі**

  Ашылмалы тізімнен келесі элементтерді таңдауға болады:

  - **Анықталмаған**.
  - **Жоқ**. Virtual Desktop Infrastructure-дың бөлігі болып табылмайтын құрылғыларды табу.
  - **Иә**. Ізделетін құрылғылар Virtual Desktop Infrastructure (VDI) бөлігі болуы тиіс.

Жабдық тізімдемесі бөлімінде құрылғыларды оларға орнатылған жабдық бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

> lshw утилитасы, жабдық туралы ақпарат алғыңыз келетін Linux құрылғыларында орнатылғанын тексеріңіз. Виртуалды машиналардан алынған жабдық туралы мәлімет пайдаланылатын гипервизорға байланысты толық болмауы мүмкін

- **Құрылғы**

  Ашылмалы тізімнен жабдық түрін таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Өндіруші**

  Ашылмалы тізімнен жабдық өндірушісінің атауын таңдауға болады. Мұндай жабдықтары бар барлық құрылғылар іздеу нәтижесіне қосылған.

  Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Құрылғы атауы**

  Windows желісіндегі құрылғының атауы. Көрсетілген атауы бар құрылғы таңдауға қосылады.

- **Сипаттама**

  Құрылғының немесе жабдықтың сипаттамасы. Өрісте көрсетілген сипаттамасы бар құрылғылар таңдау құрамына енгізіледі.

Құрылғының сипаттамасын құрылғының сипаттары терезесінде еркін түрде енгізуге болады. Өрісте толық мәтінді іздеуге қолдау көрсетіледі.

- **Құрылғы өндірушісі**

  Құрылғы өндірушісінің атауы. Өрісте көрсетілген өндіруші жасаған құрылғылар таңдау құрамына енгізіледі.

  Өндірушінің атауын құрылғының сипаттары терезесінде енгізуге болады.

- **Сериялық нөмір**

  Өрісте көрсетілген сериялық нөмірі бар жабдық таңдауға қосылады.

- **Қойма нөмірі**

  Өрісте көрсетілген қойма нөмірі бар жабдық таңдауға қосылады.

- **Пайдаланушы**

  Өрісте көрсетілген пайдаланушының аппараттық жасақтамасы таңдауға қосылады.

- **Орналасуы**

  Құрылғының немесе жабдықтың орналасқан жері (мысалы, кеңседе немесе филиалда). Өрісте көрсетілген жерде орналасқан компьютерлер немесе басқа құрылғылар таңдау құрамына кіреді.

  Жабдықтың орналасуын жабдықтың сипаттары терезесінде еркін түрде енгізуге болады.

- **Орталық процессор тактілік жиілігі, МГц түрінде, келесіден бастап**

  Процессордың ең төменгі тактілік жиілігі. Енгізу өрістерінде (қоса алғанда) көрсетілген жиіліктер ауқымына сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Орталық процессор тактілік жиілігі, МГц түрінде, осыған дейін**

  Процессордың ең жоғарғы тактілік жиілігі. Енгізу өрістерінде (қоса алғанда) көрсетілген жиіліктер ауқымына сәйкес келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Виртуалды орталық процессор ядроларының саны, басы**

  CPU виртуалды өзектерінің ең аз саны. Енгізу өрістерінде (қоса алғанда) көрсетілген виртуалды өзектер санының ауқымына келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Виртуалды орталық процессор ядроларының саны, соңы**

  CPU виртуалды өзектерінің ең көп саны. Енгізу өрістерінде (қоса алғанда) көрсетілген виртуалды өзектер санының ауқымына келетін орталық процессорлары бар құрылғылар таңдау құрамына енгізіледі.

- **Қатты дискінің көлемі, ГБ түрінде, келесіден бастап**

  Құрылғының қатты дискісінің ең аз көлемі. Енгізу өрістеріндегі (қоса алғанда) мәндер ауқымына сәйкес келетін қатты дискілері бар құрылғылар таңдау құрамына енгізіледі.

- **Қатты дискінің көлемі, ГБ түрінде, келесіге дейін**

  Құрылғының қатты дискісінің ең көп көлемі. Енгізу өрістеріндегі (қоса алғанда) мәндер ауқымына сәйкес келетін қатты дискілері бар құрылғылар таңдау құрамына енгізіледі.

- **Жедел жад өлшемі, МБ түрінде, келесіден бастап**

  Құрылғы ЖЖҚ-сының минималды өлшемі. Енгізу өрістерінде (қоса алғанда) көрсетілген өлшем ауқымына сәйкес келетін ЖЖҚ-сы бар құрылғылар таңдауға қосылады.

- **Жедел жад өлшемі, МБ түрінде, келесіге дейін**

  Құрылғы ЖЖҚ-сының максималды өлшемі. Енгізу өрістерінде (қоса алғанда) көрсетілген өлшем ауқымына сәйкес келетін ЖЖҚ-сы бар құрылғылар таңдауға қосылады.

Үшінші тарап бағдарламалық жасақтамасы туралы мәліметтер

Бағдарламалар тізімдемесі бөлімінде қандай бағдарламалар орнатылғанына байланысты құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Бағдарламаны таңдауға болатын ашылмалы тізім. Көрсетілген бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарламаның нұсқасы**

  Таңдалған бағдарламаның нұсқасын көрсететін енгізу өрісі.

- **Өндіруші**

  Құрылғыда орнатылған бағдарламаның өндірушісін таңдауға болатын ашылмалы тізім.

- **Бағдарлама күйі**

  Бағдарлама күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған бағдарлама орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

- **Жаңарту бойынша іздеу**

  Егер бұл параметр қосулы болса, іздеу сіз іздеген құрылғыларда орнатылған бағдарламаларды жаңарту деректері бойынша орындалады. Жалауша қойылғаннан кейін, **Бағдарлама атауы**, **Бағдарламаның нұсқасы** және **Бағдарлама күйі** өрістерінің орнына сәйкесінше **Жаңартудың атауы**, **Жаңартудың нұсқасы** және **Күйі** өрістері көрсетіледі.

  Әдепкі бойынша, параметр өшірулі.

- **Үйлесімсіз қауіпсіздік бағдарламасының аты**

  Үшінші тарап қауіпсіздік бағдарламаларын таңдауға болатын ашылмалы тізім. Іздеу кезінде, таңдалған бағдарлама орнатылған құрылғылар таңдауға қосылады.

- **Бағдарлама тегі**

  Ашылмалы тізімнен бағдарлама тегін таңдауға болады. Сипаттамада таңдалған тегі бар бағдарламалар орнатылған барлық құрылғылар құрылғылар таңдауына қосылады.

- **Көрсетілген тегтерсіз құрылғыларға қолдану**

  Параметр қосулы болса, онда таңдауға, сипаттамасында таңдалған тегтері жоқ құрылғылар қосылады.

  Бұл параметр өшірулі болса, өлшемшарт қолданылмайды.

  Әдепкі бойынша, параметр өшірулі.

Осалдықтар мен жаңартулар бөлімінде, құрылғыларды Windows Update жаңарту көздері бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

WUA Басқару серверіне ауысты

Ашылмалы тізімнен келесі іздеу нұсқаларының бірін таңдауға болады:

- **Иә**. Егер бұл нұсқа таңдалса, іздеу нәтижелеріне Windows Update жаңартуларын Басқару серверінен алатын құрылғылар кіреді.
- **Жоқ**. Бұл нұсқа таңдалса, нәтижелер жаңартуларды Windows Update арқылы басқа дереккөздерден алатын құрылғыларды қамтиды.

Kaspersky бағдарламалары туралы мәліметтер

Kaspersky бағдарламалары бөлімінде құрылғыларды таңдалған басқарылатын бағдарламаның негізінде таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Бағдарлама атауы**

  Ашылмалы тізімде, Kaspersky бағдарламасының атауы бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын таңдауға болады.

  Тізімде, әкімшінің жұмыс станциясында басқару плагиндері орнатылған бағдарламалардың атаулары ғана берілген.

  Егер бағдарлама таңдалмаса, онда өлшемшарт қолданылмайды.

- **Бағдарламаның нұсқасы**

  Енгізу өрісінде Kaspersky бағдарламасы нұсқасының нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер нұсқа нөмірі көрсетілмесе, онда өлшемшарт қолданылмайды.

- **Критикалық жаңартудың атауы**

  Бағдарлама күйін таңдауға болатын ашылмалы тізім (*Орнатылған*, *Орнатылмаған*). Таңдалған күйге байланысты, аталған бағдарлама орнатылған немесе орнатылмаған құрылғылар таңдауға қосылады.

  Енгізу өрісінде бағдарлама үшін белгіленген жаңарту пакетінің атауы немесе нөмірі бойынша іздеу кезінде құрылғыларды таңдау құрамына қосу өлшемшартын көрсетуге болады.

  Егер өріс толтырылмаса, онда өлшемшарт қолданылмайды.

- **Модульдердің соңғы жаңарту мерзімін таңдау**

  Бұл параметрдің көмегімен құрылғыларда орнатылған бағдарлама модульдерінің соңғы рет жаңартылған уақыты бойынша құрылғыларды іздеу өлшемшартын белгілеуге болады.

  Егер жалауша қойылса, енгізу өрістерінде құрылғыларда орнатылған бағдарлама модульдерінің соңғы жаңартылуы орындалған аралық мәндерін (күні мен уақыты) көрсетуге болады.

  Егер жалауша алынып тасталса, онда өлшемшарт қолданылмайды.

  Әдепкі бойынша, жалауша алынып тасталған.

- **Құрылғы Басқару сервері арқылы басқарылады**

  Ашылмалы тізімде Kaspersky Security Center басқаратын құрылғыларды таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама Kaspersky Security Center басқаратын құрылғыларды таңдауды қамтиды.
  - **Жоқ**. Қолданба Kaspersky Security Center арқылы басқарылмайтын құрылғыларды таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

- **Қауіпсіздік бағдарламасы орнатылған**

  Ашылмалы тізімде қауіпсіздік бағдарламасы орнатылған құрылғыны таңдау құрамына қосуға болады:

  - **Иә**. Бағдарлама, қауіпсіздік бағдарламасы орнатылған құрылғыларды таңдауға қосады.
  - **Жоқ**. Қолданба қауіпсіздік қолданбасы орнатылмаған барлық құрылғыны таңдауға қосады.
  - **Мән таңдалмаған**. Өлшемшарт қолданылмайды.

Антивирустық қорғаныс бөлімінде құрылғыларды қорғаныс күйі бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады:

- **Дерекқорлардың шығарылған күні**

  Осы параметр таңдалса, клиент құрылғыларын іздеу антивирустық дерекқордың шығарылу күні бойынша орындалады. Енгізу өрістерінде іздеу жүргізілетін уақыт аралығын белгілеуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Дерекқорлардағы жазбалар саны**

  Егер бұл параметр қосылса, клиент құрылғыларын іздеу дерекқордағы жазбалар саны бойынша жүзеге асырылады. Енгізу өрістерінде антивирустық дерекқордың жазбалары санының төменгі және жоғарғы мәндерін орнатуға болады.

  Әдепкі бойынша, параметр өшірулі.

- **Вирустарға соңғы рет тексеру уақыты**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу соңғы рет зиянды БҚ іздеу уақыты бойынша жүзеге асырылады. Енгізу өрістерінде зиянды БҚ іздеу соңғы рет жүргізілген аралықты көрсетуге болады.

  Әдепкі бойынша, параметр өшірулі.

- **Қауіптер анықталды**

  Егер бұл параметр қосулы болса, клиент құрылғыларын іздеу табылған вирустар санына сәйкес жүзеге асырылады. Енгізу өрістерінде табылған вирустар санының төменгі және жоғарғы мәндерін орнатуға болады.

  Әдепкі бойынша, параметр өшірулі.

Шифрлау бөлікшесінде таңдалған шифрлау алгоритмі негізінде таңдауға құрылғыларды қосу критерийлерін конфигурациялауға болады:

Шифрлау алгоритмі

Advanced Encryption Standard (AES) симметриялық блоктық шифрлау алгоритмі стандарты. Ашылмалы тізімнен шифрлау кілтінің өлшемін таңдай аласыз (56 Бит, 128 Бит, 192 Бит немесе 256 Бит).

Қолжетімді мәндер: *AES56*, *AES128*, *AES192*, және *AES256*.

Бағдарлама құрамдастары бөлікшесі Kaspersky Security Center Web Console веб-консолінде сәйкес басқару плагиндері орнатылған қолданба құрамдастарының тізімін қамтиды.

Бағдарлама құрамдастары қойыншасында, таңдалған бағдарламаға қатысты құрамдастар нұсқаларының нөмірлеріне сәйкес құрылғыларды іріктеуге қосу өлшемшартын белгілеуге болады:

- **Күйі**

  Басқарылатын бағдарлама Басқару серверіне жіберген құрамдастың күйіне сәйкес құрылғыларды іздеу. Келесі күйлердің бірін таңдауға болады: *Құрылғыдан деректер жоқ*, *Тоқтатылды*, *Кідіртілді*, *Іске қосулы*, *Орындалуда*, *Сәтсіз аяқталды*, *Орнатылмаған*, *Лицензия қолдау көрсетпейді*. Егер басқарылатын құрылғыда орнатылған бағдарламаның таңдалған құрамдасы көрсетілген күйге ие болса, құрылғы құрылғыны таңдауға кіреді.

  Бағдарламалар жіберген күйлер:

  - *Тоқтатылды* – құрамдас өшірілген және қазіргі уақытта жұмыс істемейді.
  - *Кідіртілді* – құрамдас, мысалы, пайдаланушы басқарылатын бағдарламада қорғанысты кідірткеннен кейін кідіртіледі.
  - *Іске қосылды* – құрамдас қазіргі уақытта инициализация процесінде.
  - *Орындалуда* – құрамдас қосулы және дұрыс жұмыс істейді.
  - *Сәтсіз аяқталды* – құрамдастың операциясын орындау кезінде қате пайда болды.
  - *Орнатылмаған* – пайдаланушы бағдарламаны іріктеп орнату кезінде орнату құрамдасын таңдамады.
  - *Лицензия қолдау көрсетпейді* - Лицензия таңдалған құрамдасқа қолданылмайды.

  Басқа күйлерден айырмашылығы, *Құрылғыдан деректер жоқ* күйін басқарылатын бағдарлама жібермейді. Бұл параметр, бағдарламаларда таңдалған құрамдас күйі туралы ақпарат жоқ екенін көрсетеді. Мысалы, бұл жағдай, таңдалған құрамдас құрылғыда орнатылған бағдарламалардың ешқайсысына тиесілі болмаса немесе құрылғы өшірулі болса, орын алуы мүмкін.

- **Нұсқа**

  Тізімде таңдалған құрамдас нұсқасының нөміріне сәйкес құрылғыларды іздеу. Сіз `3.4.1.0` сияқты нұсқа нөмірін енгізе аласыз, содан кейін таңдалған құрамдастың тең, анағұрлым ерте немесе анағұрлым кейінгі нұсқасы болуы керек пе екенін көрсете аласыз. Сондай-ақ, іздеуді көрсетілген нұсқадан басқа құрамдастың барлық нұсқалары бойынша конфигурациялауға болады.

Тегтер

Тегтер бөлімінде бұған дейін басқарылатын құрылғылардың сипаттамаларына қосылған кілт сөздер (тегтер) бойынша құрылғыларды таңдауға қосу өлшемшарттарын конфигурациялауға болады:

Кем дегенде бір көрсетілген тег сәйкес келген жағдайда қолдану

Егер бұл параметр қосулы болса, іздеу нәтижелерінде сипаттамасында таңдалған тегтердің кемінде біреуі бар құрылғылар көрсетіледі.

Егер бұл параметр өшірулі болса, іздеу нәтижелерінде тек сипаттамаларында барлық таңдалған тегтері бар құрылғылар көрсетіледі.

Әдепкі бойынша, параметр өшірулі.

Критерийге тегтерді қосу үшін **Қосу** түймесін басыңыз және **Тег** енгізу өрісін басу арқылы тегтерді таңдаңыз. Құрылғы таңдауында таңдалған тегтері бар құрылғыларды қосу немесе алып тастау керектігін көрсетіңіз.

- **Бұл тег бар барлық құрылғылар**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі бар құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Бұл тег жоқ барлық құрылғылар**

  Егер бұл нұсқа таңдалса, іздеу нәтижелерінде сипаттамасында таңдалған тегі жоқ құрылғылар көрсетіледі. Құрылғыларды іздеу үшін 0 немесе одан да ұзын таңбалардан тұратын кез келген жолды ауыстыратын * таңбасын пайдалануға болады.

Пайдаланушылар

Пайдаланушылар бөлімінде құрылғыларды операциялық жүйеге кірген пайдаланушылардың есептік жазбалары бойынша таңдауға қосу өлшемшарттарын конфигурациялауға болады.

- **Жүйеге соңғы кірген пайдаланушы**

  Бұл параметр қосылса, критерийді конфигурациялаған пайдаланушы есептік жазбасын таңдауға болады. Іздеу нәтижелеріне, жүйеге соңғы рет кіруді таңдалған пайдаланушы орындаған құрылғылар кіреді.

- **Жүйеге кемінде бір рет кірген пайдаланушы**

  Егер бұл параметр қосылса, **Шолу** түймесін басқан кезде пайдаланушы есептік жазбасын көрсетуге болады. Іздеу нәтижелеріне, аталған пайдаланушы жүйеге кемінде бір рет кірген құрылғылар кіреді.

Құрылғы таңдауларынан құрылғылар тізімін экспорттау

Kaspersky Security Center жүйесі бұл құрылғылар туралы ақпаратты құрылғы таңдауынан сақтауға және CSV немесе TXT файлына экспорттауға мүмкіндік береді.

Құрылғы таңдауынан құрылғылар тізімін экспорттау үшін:

1. Құрылғы таңдауынан құрылғылары бар кестені ашыңыз.
2. Экспорттағыңыз келетін құрылғыларды таңдау үшін келесі әдістердің бірін пайдаланыңыз:
   - Нақты бір құрылғыларды таңдау үшін олардың жанындағы жалаушаларды белгілеңіз.
   - Ағымдағы кесте бетіндегі барлық құрылғыларды таңдау үшін құрылғы кестесінің тақырыбында жалаушаны белгілеп, **Ағымдағы бетте барлығын таңдау** жалаушасын белгілеңіз.
   - Кестеден барлық құрылғыларды таңдау үшін құрылғы кестесінің тақырыбында жалаушаны белгілеп, **Барлығын таңдау** опциясын таңдаңыз.
3. **CSV файлына экспорттау** немесе **TXT файлына экспорттау** түймесін басыңыз. Кестеге енгізілген таңдалған құрылғылар туралы барлық ақпарат экспортталады.

Құрылғы кестесін сүзген болсаңыз, тек көрсетілген бағандардың сүзілген деректері экспортталатынын ескеріңіз.

Таңдаудағы басқару топтарынан құрылғыларды жою

Құрылғы үлгісімен жұмыс істегенде, құрылғыларды жою қажет басқару топтарымен жұмыс істеуге өтпей-ақ, құрылғыларды басқару топтарынан тікелей таңдаудың өзінде жоюға болады.

Басқару топтарынан құрылғыларды жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Құрылғы таңдаулары** немесе **Табу және орналастыру** → **Құрылғы таңдаулары** бөліміне өтіңіз.
2. Таңдаулар тізімінде құрылғыны таңдаудың атауын басыңыз.

   Бетте құрылғы таңдауына енгізілген құрылғылар туралы ақпараты бар кесте көрсетілген.
3. Жойғыңыз келетін құрылғыларды таңдап, **Жою** түймесін басыңыз.

   Нәтижесінде, таңдалған құрылғылар өздері кіретін басқару топтарынан жойылады.

Құрылғы тегтері

Kaspersky Security Center құрылғыларға *тегтерді* тағайындауға мүмкіндік береді. Тег дегеніміз – құрылғыларды топтау, сипаттау, іздеу үшін пайдалануға болатын құрылғы идентификаторы. Құрылғыларға тағайындалған тегтер, құрылғылар іріктемесін жасау, құрылғыларды іздеу және құрылғыларды басқару топтары бойынша бөлу кезінде пайдаланылуы мүмкін.

Тегтерді құрылғыларға қолмен немесе автоматты түрде тағайындауға болады. Бөлек құрылғыны белгілегіңіз келсе, тегті қолмен тағайындауға болады. Автоматты түрде тэгті тағайындауды Kaspersky Security Center келесі тәсілдердің бірімен орындайды:

- Көрсетілген тег тағайындау ережелеріне сәйкес.
- Көрсетілген қолданбаға сәйкес.

Бір тегті тағайындау үшін тегтерді тағайындаудың әртүрлі тәсілдерін қолдану ұсынылады. Мысалы, тег ереже арқылы тағайындалса, ол тегті құрылғыларға қолмен тағайындау ұсынылмайды.

Тэгтерді ережелер тағайындаса, берілген ережелер орындалса, құрылғыларға тэгтер автоматты түрде тағайындалады. Әрбір тегке бөлек ереже сай келеді. Ережелер құрылғының желілік сипаттарына, операциялық жүйеге, құрылғыда орнатылған бағдарламаларға және құрылғының басқа да сипаттарына қатысты қолданылуы мүмкін. Мысалы, физикалық құрылғылардан, Amazon EC2 даналарынан және Microsoft Azure виртуалды машиналарынан тұратын гибридті инфрақұрылым пайдаланылса, барлық Microsoft Azure виртуалды машиналарына `[Azure]` тегі тағайындалатын ережені конфигурациялауға болады. Содан кейін, бұл тегті, барлық Microsoft Azure виртуалды машиналарын таңдап, оларға тапсырма беру үшін құрылғы таңдауын жасау кезінде пайдалануға болады.

Әрбір тэгке бір ғана автоматты тэг енгізу ережесін қосуға болады. Бір тэг үшін жаңа ереже жасасаңыз, алдыңғысы ауыстырылады.

Тег келесі жағдайларда құрылғыдан автоматты түрде жойылады:

- Құрылғы тегті белгілеу ережелерінің шарттарын қанағаттандыруды тоқтатады.
- Тегті белгілеу ережесі өшірулі немесе қосулы.

Әрбір Басқару серверіне арналған тегтер мен ережелер тізімдері барлық Басқару серверлері, соның ішінде негізгі Басқару сервері және қосалқы виртуалды Басқару серверлері үшін тәуелсіз болып саналады. Ереже тек өзі жасалған Басқару серверінің басқаруымен жұмыс істейтін құрылғыларға ғана қолданылады.

Құрылғы тегтерін жасау

Құрылғының тегін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Тег жасау терезесі көрсетіледі.
3. **Тег** өрісінде тег атауын енгізіңіз.
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жаңа жасалған тег құрылғы тегтерінің тізімінде пайда болады.

Құрылғы тегтерін өзгерту

Құрылғының тегін қайта атау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. Қайта атау қажет болған тегті бөлектеңіз.

   Тегтің сипаттары терезесі ашылады.
3. **Тег** өрісінде тегтің атауын өзгертіңіз.
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жаңартылған тег құрылғы тегтері тізімінде пайда болады.

Құрылғы тегтерін жою

Құрылғы тегтерін жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. Тізімнен жойғыңыз келетін құрылғы тегтерін таңдаңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **Иә** түймесін басыңыз.

Құрылғының таңдалған тегі жойылды. Жойылған тег, ол тағайындалған барлық құрылғылардан автоматты түрде алынып тасталады.

Сіз жойған тег, автоматты түрде тег қою ережелерінен автоматты түрде жойылмайды. Тегті жойғаннан кейін, ол құрылғының параметрлері тегтерді белгілеу ережелерінің шарттарына бірінші рет сай келген кезде жаңа құрылғыға тағайындалатын болады.

Егер бұл тег құрылғыға бағдарлама немесе Желілік агент арқылы тағайындалса, жойылған тег құрылғыдан автоматты түрде жойылмайды. Бұл тегтерді басқару үшін klscflag утилитасын пайдаланыңыз.

Тег тағайындалған құрылғыларды қарап шығу

Тегтері тағайындалған құрылғыларды қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері** бөліміне өтіңіз.
2. Тағайындалған құрылғылар тізімін қарағыңыз келетін құрылғы үшін тег атауының жанындағы **Құрылғыларды көру** сілтемесінен өтіңіз.

   Сіз **Басқарылатын құрылғылар** сілтемесін басқан тег бойынша сүзілген құрылғылары бар негізгі мәзірдің **Құрылғыларды көру** бөліміне қайта бағытталасыз.
3. Құрылғы тегтерінің тізіміне оралу үшін браузердегі **Артқа** түймесін басыңыз.

Тағайындалған тегі бар құрылғыларды көргеннен кейін, сіз жаңа тег жасап, тағайындай аласыз немесе бар тегті басқа құрылғыларға тағайындай аласыз. Бұл жағдайда, сүзгіні тег бойынша алып тастауға, құрылғыларды таңдауға және тегті тағайындауға тура келеді.

Құрылғыға тағайындалған тегтерді қарап шығу

Құрылғыға тағайындалған тегтерді қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Тегтерін қарап шығу қажет құрылғыны таңдаңыз.
3. Ашылған құрылғы сипаттары терезесінде **Тегтер** қойыншасын таңдаңыз.

   Таңдалған құрылғыға тағайындалған тегтер тізімі көрсетіледі. **Тег белгіленді** бағанында тегтің қалай тағайындалғанын көруге болады.

Құралдар тақтасында келесі әрекеттерді орындауға болады:

- Құрылғыға басқа тэгті тағайындау.
- Бұрыннан тағайындалған тэгті өшіру.
- Басқару серверінде бар барлық құрылғы тэгтерін көру.

> Тағайындалған тэгтерді құрылғыдан жергілікті түрде көру мүмкін емес.

Құрылғыға тегтерді қолмен тағайындау

Құрылғыға тегті қолмен тағайындау үшін:

1. Тег тағайындағыңыз келетін құрылғыға тағайындалған тегтерді қарап шығыңыз.
2. **Қосу** түймесін басыңыз.

3. Ашылған терезеде келесі әрекеттердің бірін орындаңыз:

   - Жаңа тегті жасау және қосу үшін **Жаңа тегті жасау** тармағын таңдап, тег атауын көрсетіңіз.
   - Қолданыстағы тегті таңдау үшін, **Бар тегті тағайындау** тармағын таңдап, ашылмалы тізімнен қажетті тегті таңдаңыз.

4. Өзгерістерді қолдану үшін **ОК** түймесін басыңыз.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған тег құрылғыға тағайындалады.

Тағайындалған тегті құрылғыдан жою

Құрылғыдан тағайындалған тегті алып тастау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

2. Тегтерін қарап шығу қажет құрылғыны таңдаңыз.

3. Ашылған құрылғы сипаттары терезесінде **Тегтер** қойыншасын таңдаңыз.

4. Алып тастау қажет тегке қарама қарсы жалауша қойыңыз.

5. Тізімнің жоғарғы жағындағы **Тегті тағайындаудан алу қажет пе?** түймесін басыңыз.

6. Пайда болған терезеде **Иә** түймесін басыңыз.

Тег құрылғыдан алып тасталады.

Құрылғыдан алынған тег жойылмайды. Қажет болса, оны қолмен жоюға болады.

Бағдарламалар немесе Желілік агент арқылы құрылғыға тағайындалған тегтерді қолмен жою мүмкін емес. Бұл тегтерді басқару үшін klscflag утилитасын пайдаланыңыз.

Құрылғыларға автоматты түрде тег қою ережелерін қарап шығу

Құрылғыларға автоматты түрде тег қою ережелерін қарап шығу үшін,

Келесі әрекеттердің бірін орындаңыз:

- Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Автоматты түрде тег қою ережелері** бөліміне өтіңіз.
- Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тегтер** → **Құрылғы тегтері**, содан соң **Автоматты түрде тег қою ережелерін орнату** сілтемесінен өтіңіз.
- Құрылғыға тағайындалған тегтерді қараңыз, сосын **Автоматты түрде тег қою ережелерін орнату** түймесін басыңыз.

Құрылғыларға автоматты түрде тег қою ережелері тізімі көрсетіледі.

Құрылғыларға автоматты түрде тег қою ережелерін өзгерту

Құрылғыларға автоматты түрде тег қою ережелерін өзгерту үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.
2. Өзгерту қажет ережені таңдаңыз.

   Ереже параметрлері бар терезе ашылады.
3. Ереженің негізгі параметрлерін өзгертіңіз:

   a. **Ереженің атауы** өрісінде ереженің атауын өзгертіңіз.

   Атауы 256 таңбадан аспауы керек.

   b. Келесі әрекеттердің бірін орындаңыз:

   - Қосқышты **Ереже қосулы** күйіне қойып, ережені қосыңыз.
   - Қосқышты **Ереже өшірулі** күйіне қойып, ережені өшіріңіз.
4. Келесі әрекеттердің бірін орындаңыз:

   - Жаңа шартты қосқыңыз келсе, **Қосу** түймесін басыңыз және ашылған терезеде жаңа шарттың параметрлерін көрсетіңіз.
   - Егер сіз қолданыстағы шартты өзгерткіңіз келсе, өзгертуді қажет ететін шартты бөлектеңіз және оның параметрлерін өзгертіңіз.
   - Егер сіз шартты жойғыңыз келсе, жойылатын шарт атауының жанына жалаушаны қойып, **Жою** түймесін басыңыз.

5. Шарт параметрлері терезесінде **OK** түймесін басыңыз.

6. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Өзгертілген ереже тізімде көрсетіледі.

Құрылғыларға автоматты түрде тег қою ережелерін жасау

Құрылғыларға автоматты түрде тег қою ережелерін жасау үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.

2. **Қосу** түймесін басыңыз.

   Жаңа ереже параметрлері бар терезе ашылады.

3. Ереженің негізгі параметрлерін көрсетіңіз:

   a. **Ереженің атауы** өрісінде ереженің атауын енгізіңіз.

      Атауы 256 таңбадан аспауы керек.

   b. Келесі әрекеттердің бірін орындаңыз:

      - Қосқышты **Ереже қосулы** күйіне қойып, ережені қосыңыз.
      - Қосқышты **Ереже өшірулі** күйіне қойып, ережені өшіріңіз.

   c. **Тег** өрісінде құрылғы тегінің жаңа атауын көрсетіңіз немесе тізімнен қолданыстағы құрылғы тегін таңдаңыз.

      Атауы 256 таңбадан аспауы керек.

4. Шартты таңдау өрісінде, жаңа шартты қосу үшін **Қосу** түймесін басыңыз.

   Жаңа шарт параметрлері бар терезе ашылады.

5. Шарттың атауын көрсетіңіз.

   Атауы 256 таңбадан аспауы керек. Шарттың атауы бір ереже шеңберінде бірегей болуы керек.

6. Ереженің іске қосылуын келесі шарттар бойынша конфигурациялаңыз. Бірнеше шарт таңдауға болады.

   - **Желі** – құрылғының желілік қасиеттері (мысалы, Windows желісіндегі құрылғының атауы, құрылғының доменге немесе IP ішкі желісіне жатуы).

     > Kaspersky Security Center үшін пайдаланып жатқан дерекқорда тіркелімді ескере отырып сұрыптау конфигурацияланған болса, құрылғының DNS атауын көрсеткенде тіркемді ескеріңіз. Әйтпесе, автоматты түрде тег қою ережелері жұмыс істемейді.

   - **Бағдарламалар** – құрылғыда Желілік агенттің болуы, операциялық жүйенің түрі, нұсқасы және архитектурасы.

   - **Виртуалды машиналар** – құрылғының виртуалды машиналардың белгілі бір түріне тиесілі болуы.

- **Домен контроллері** – құрылғының Active Directory бөлімшесінде болуы және құрылғының Active Directory тобына мүшелігі.
- **Бағдарламалар тізімдемесі** – құрылғыда әртүрлі өндірушілердің бағдарламаларының болуы.

7. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

   Қажет болса, бір ереже үшін бірнеше шарт белгілеуге болады. Бұл жағдайда, құрылғылар үшін шарттардың кемінде біреуі орындалса, тег оларға тағайындалады.

8. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жасалған ереже, таңдалған Басқару сервері басқаратын құрылғыларда орындалады. Құрылғы параметрлері ереженің шарттарына сәйкес келсе, бұл құрылғыға тег тағайындалады.

Алдағыда, ереже келесі жағдайларда қолданылады:

- Сервердің жүктелуіне байланысты, автоматты түрде, үнемі.
- Ережені өзгерткеннен кейін.
- Ережені қолмен орындағаннан кейін.
- Басқару сервері ереже шарттарына сәйкес келетін өзгерістерді құрылғы параметрлерінде немесе осы құрылғыны қамтитын топ параметрлерінде анықтағаннан кейін.

Сіз бірнеше тег тағайындау ережесін жасай аласыз. Бірнеше тег тағайындау ережесін жасаған болсаңыз және осы ережелердің шарттары бір уақытты орындалып жатса, бір құрылғыға бірнеше тег тағайындалуы мүмкін. Барлық тағайындалған тегтер тізімін құрылғының сипаттарында қарап шыға аласыз.

Құрылғыларға автоматты түрде тег қою ережелерін орындау

Ереже орындалған кезде, осы ереженің сипаттарында көрсетілген тег ереженің сипаттарында көрсетілген шарттарға сәйкес келетін құрылғыға тағайындалады. Тек белсенді ережелерді орындауға болады.

Құрылғыларға автоматты түрде тег қою ережелерін орындау үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.
2. Орындалатын белсенді ережелерге қарама-қарсы жалаушаларды қойыңыз.
3. **Іске қосу ережесі** түймесін басыңыз.

Таңдалған ережелер орындалады.

Құрылғылардан автоматты түрде тег қою ережелерін жою

Құрылғыларға автоматты түрде тег қою ережелерін жою үшін:

1. Құрылғыларға автоматты түрде тег қою ережелерін қарап шығыңыз.
2. Жойғыңыз келетін ережеге қарама-қарсы жалаушаны қойыңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **Жою** түймесін тағы да басыңыз.

Таңдалған ереже жойылады. Осы ереженің сипаттарында көрсетілген тег тағайындалған барлық құрылғылардан алынады.

Құрылғыдан алынған тег жойылмайды. Қажет болса, оны қолмен жоюға болады.

klscflag утилитасы арқылы құрылғылар тегтерін басқару

Құрылғыға тэгтер жинағын тағайындау үшін тэгтерді тағайындағыңыз келетін клиент құрылғысында klscflag утилитасын іске қосу керек.

Klscflag утилитасы құрылғыға тағайындалған бар тэгтерді қайта жазады. Бұл пәрмендегі қажетті тэгтер жинағын көрсету арқылы тэгтерді қосуға немесе өшіруге болатынын білдіреді. Утилитада жеке тэгтерді қосу немесе өшіру үшін бөлек пәрмендер жоқ. Оның орнына сіз тэгтердің бүкіл жинағын өзгертесіз.

klscflag сияқты пәрмендердегі тэг атауларын көрсеткен кезде, барлығын бас әріппен алу сияқты бірдей әріп әдісін пайдаланған жөн. Барлығын бас әріппен қолдану арқылы ДҚБЖ конфигурациясына байланысты тек әрпі өзгеше тэгтерге қатысты ықтимал мәселелерге жол бермеуге көмектеседі.

klscflag утилитасын пайдаланып, құрылғыңызға тэгтерді тағайындау үшін:

1. Әкімші құқықтары бар Windows пәрмен жолын іске қосыңыз, содан кейін ағымдағы каталогті klscflag утилитасы бар каталогке өзгертіңіз. klscflag утилитасы Желілік агенттің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Келесі пәрмендердің бірін енгізіңіз:

   - Тэгтер жинағын тағайындау үшін:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ 2\",\"ТЕГ АТАУЫ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     мұндағы `[\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ 2\",\"ТЕГ АТАУЫ 3\"]` — құрылғыға тағайындағыңыз келетін тэгтер тізімі.

     Шаршы жақшаларды бос қалдырсаңыз, құрылғыдан барлық тэгтер жойылады:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - Бар тэгтер жинағына жаңа тэг тағайындау үшін:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ЖАҢА ТЕГ АТАУЫ\",\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ 2\",\"ТЕГ АТАУЫ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     мұндағы `ЖАҢА ТЕГ АТАУЫ` is the name of the tag that you want to assign to your device and `ТЕГ АТАУЫ 1`, `ТЕГ АТАУЫ 2`, `ТЕГ АТАУЫ 3` — құрылғыға бұрыннан тағайындалған тэгтердің атаулары.

   - Құрылғыға бұрыннан тағайындалған басқа тэгтерді жоймай, белгілі бір тэгті жою үшін пәрменді тэгтердің жаңартылған жинағымен іске қосыңыз.

Мысалы, ағымдағы тегтеріңіз `ТЕГ АТАУЫ 1`, `ТЕГ АТАУЫ 2`, `ТЕГ АТАУЫ 3` болса және `ТЕГ АТАУЫ 2` тэгін өшіргіңіз келсе, келесі пәрменді орындаңыз:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv
"[\"ТЕГ АТАУЫ 1\",\"ТЕГ АТАУЫ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

3. Желілік агент қызметін қайта іске қосыңыз.

   Klscflag утилитасы құрылғыға көрсетілген тэгтерді тағайындайды.

4. klscflag утилитасы берілген тэгтерді сәтті тағайындағанына көз жеткізу үшін құрылғыға тағайындалған тэгтерді көріңіз.

Сондай-ақ, құрылғылардың тегтерін қолмен тағайындауға болады.

Саясаттар және профильдер

Kaspersky Security Center Web Console бағдарламасында Kaspersky бағдарламаларына арналған саясаттарды жасауға болады. Бұл бөлімде саясаттар және профильдер сипатталған, сондай-ақ оларды жасау және өзгерту бойынша нұсқаулар келтірілген.

Саясаттар мен саясат профильдері туралы

Саясат — басқару тобы мен оның ішкі топтарына қолданылатын Kaspersky қолданбасы параметрлерінің жиынтығы. Kaspersky бағдарламаларының бірнешеуін басқару тобының құрылғыларына орната аласыз. Kaspersky Security Center бағдарламасы басқару тобындағы Kaspersky бағдарламасының әрқайсысы үшін бір саясаттан ұсынады. Саясаттың келесі күйлерінің бірі бар (төмендегі кестені қараңыз):

Саясат күйі

Күй	Сипаттамасы
Белсенді	Бұл, құрылғыға қатысты қолданылатын ағымдағы саясат. Kaspersky бағдарламасы үшін әрбір басқару тобында тек бір саясат белсенді болуы мүмкін. Kaspersky бағдарламасының белсенді саясаты параметрлерінің мәндері құрылғыға қатысты қолданылады.
Белсенді емес	Қазіргі уақытта құрылғыға қатысты қолданылмайтын саясат.
Автономды пайдаланушылар үшін	Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.

Саясаттар келесі ережелер бойынша әрекет етеді:

- Бір бағдарлама үшін түрлі мәндері бар бірнеше саясатты конфигурациялауға болады.
- Бір бағдарлама үшін тек бір саясат белсенді болуы мүмкін.
- Белгілі бір оқиға туындаған кезде, белсенді емес саясатты белсендіре аласыз. Мысалы, вирустық шабуыл кезеңінде күшейтілген антивирустық қорғаныс үшін параметрлерді қоса аласыз.
- Саясаттың еншілес саясаттары болуы мүмкін.

Сіз вирустық шабуыл сияқты төтенше жағдайларға дайындалу үшін саясатты қолдана аласыз. Мысалы, USB флеш-дискілері арқылы шабуыл орын алса, флеш-дискілерге қатынасуға тыйым салатын саясатты іске қосуға болады. Бұл жағдайда, ағымдағы белсенді саясат автоматты түрде белсенді емес болады.

Көптеген саясаттарды қолдамау үшін, мысалы, әртүрлі жағдайларда бірнеше параметрлерді ғана өзгерту қажет болғанда, сіз саясат профильдерін қолдана аласыз.

Саясат профилі – саясат параметрлерін алмастыратын аталған саясат параметрлері ішкі жиынтығы. Саясат профилі басқарылатын құрылғының тиімді параметрлерін қалыптастыруға әсер етеді. *Тиімді параметрлер* – қазіргі уақытта құрылғыға қатысты қолданылатын саясат параметрлері, саясат профилі параметрлері және жергілікті бағдарлама параметрлері жиынтығы.

Саясат профильдері келесі ережелер бойынша жұмыс істейді:

- Саясат профилі белгіленген белсендіру шарты туындаған кезде күшіне енеді.
- Саясат профильдері саясат параметрлерінен ерекшеленетін параметр мәндерін қамтиды.
- Саясат профилін белсендіру кезінде басқарылатын құрылғының тиімді параметрлері өзгереді.
- Саясатта ең көбі 100 профиль болуы мүмкін.

Бұғаттау (құлып) және бұғатталған параметрлер

Әрбір саясат параметрінде (🔒) құлып белгішесі бар. Төмендегі кестеде құлып белгішесінің күйлері көрсетілген:

Құлып белгішесінің күйлері

Күй	Сипаттамасы
🔒 Анықталмаған	Егер параметрдің жанында ашық құлып белгішесі пайда болса және қосқыш өшірулі болса, параметр саясатта көрсетілмейді. Пайдаланушы бұл параметрлерді басқарылатын бағдарлама интерфейсінде өзгерте алады. Мұндай параметрлер *құлпы ашылған* деп аталады.
🔒 Мәжбүрлеу	Егер параметрдің жанында жабық құлып белгішесі көрсетілсе және қосқыш қосулы болса, параметр саясат қолданылатын құрылғыларға қолданылады. Пайдаланушы басқарылатын бағдарлама интерфейсіндегі осы параметрлердің мәндерін өзгерте алмайды. Мұндай параметрлер *құлыпталған* деп аталады.

Басқарылатын құрылғыларға қолданғыңыз келетін саясат параметрлерін құлыптау ұсынылады. Құлпы ашылған саясат параметрлері басқарылатын құрылғыдағы Kaspersky бағдарламасының параметрлерімен қайта тағайындалуы мүмкін.

Келесі әрекеттерді орындау үшін құлып белгішесін пайдалануға болады:

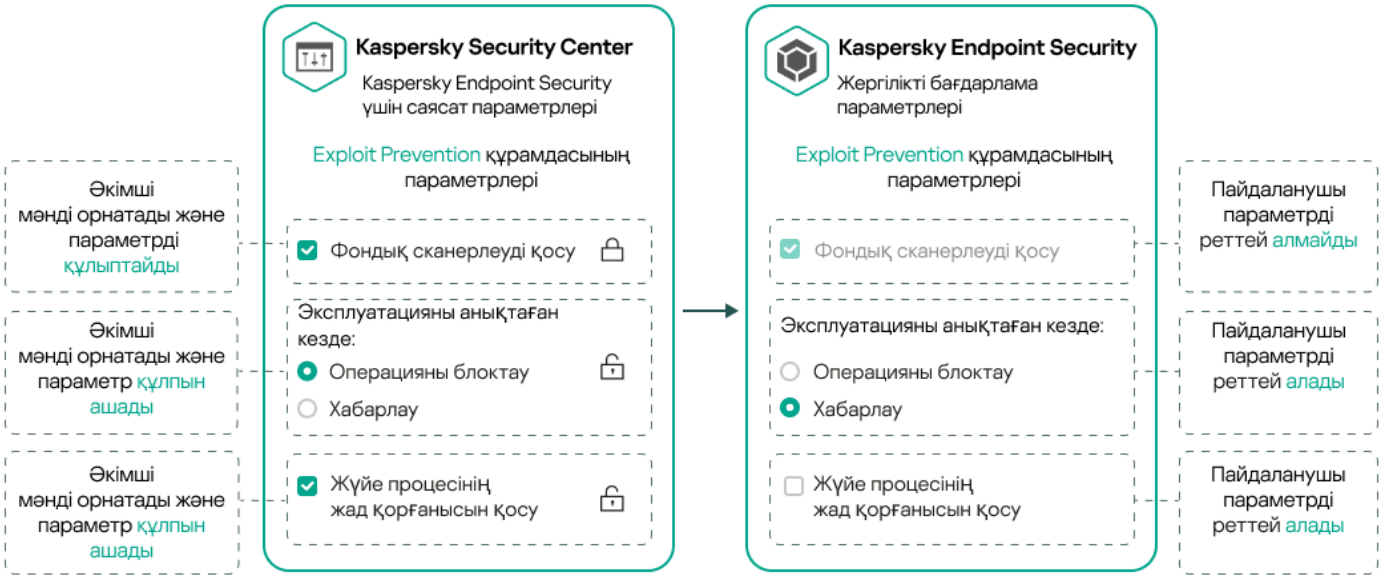
- Басқару ішкі тобы саясаты үшін параметрлерді құлыптау.
- Басқарылатын құрылғыдағы Kaspersky бағдарламасының параметрлерін құлыптау.

Осылайша, құлыпталған параметр басқарылатын құрылғыдағы тиімді параметрлерде қолданылады.

Тиімді параметрлерді қолдану келесі әрекеттерді қамтиды:

- Басқарылатын құрылғы Kaspersky бағдарламасының параметрлерінің мәндерін қолданады.
- Басқарылатын құрылғы саясат параметрлерінің құлыпталған мәндерін қолданады.

Саясат және Kaspersky басқарылатын бағдарламасы бірдей параметрлер жиынтығын қамтиды. Саясат параметрлерін конфигурациялау кезінде Kaspersky бағдарламасының параметрлері басқарылатын құрылғыдағы мәндерді өзгертеді. Басқарылатын құрылғыда құлыпталған параметрлерді өзгерту мүмкін емес (төмендегі суретті қараңыз):



Kaspersky бағдарламасының құлыптары мен параметрлері

Саясат пен саясат профильдерін иелену

Бұл бөлімде, саясаттар және профильдер иерархиясы және оларды иелену туралы ақпарат келтірілген.

Саясаттар иерархиясы

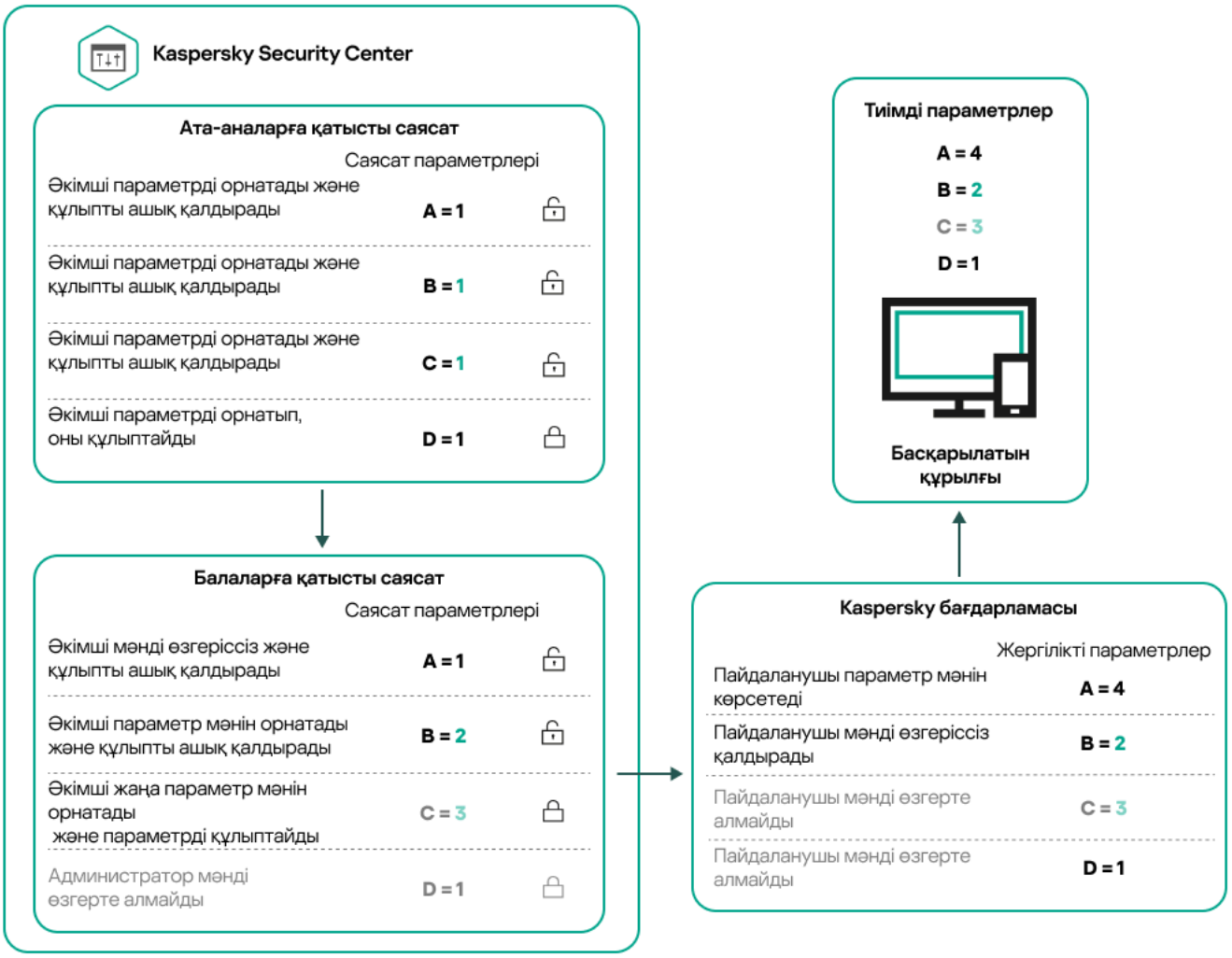
Түрлі құрылғылар үшін түрлі параметрлер керек болса, сіз құрылғыларды басқару топтарына біріктіре аласыз.

Сіз бөлек басқару тобына арналған саясатты көрсете аласыз. Саясат параметрлерін *мұралауға* болады. Иелену – (тектік) басқару тобының жоғары тұрған саясатынан ішкі топтарда (еншілес топтарда) саясат параметрлері мәндерін алу.

Тектік топ үшін жасалған саясат *тектік саясат* деп те аталады. Ішкі топ (еншілес топ) үшін жасалған саясат *еншілес саясат* деп те аталады.

Әдепкі бойынша, Басқару серверінде басқарылатын құрылғылардың кемінде бір басқару тобы бар. Егер сіз басқару топтарын құрғыңыз келсе, олар Басқарылатын құрылғылар тобында ішкі топтар (еншілес топтар) ретінде құрылады.

Бір бағдарламаның саясаттары басқару топтарының иерархиясы бойынша бір-біріне әсер етеді. Жоғары тұрған (тектік) басқару тобының саясатынан бұғатталған параметрлер ішкі топтың саясат параметрлерінің мәндерін қайта тағайындайды (төмендегі суретті қараңыз).

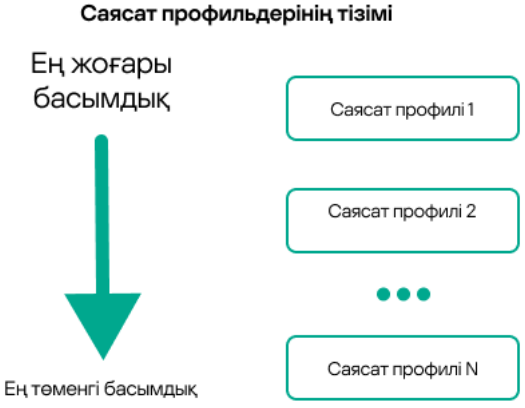


Саясаттар иерархиясы

Саясаттар иерархиясындағы саясат профильдері

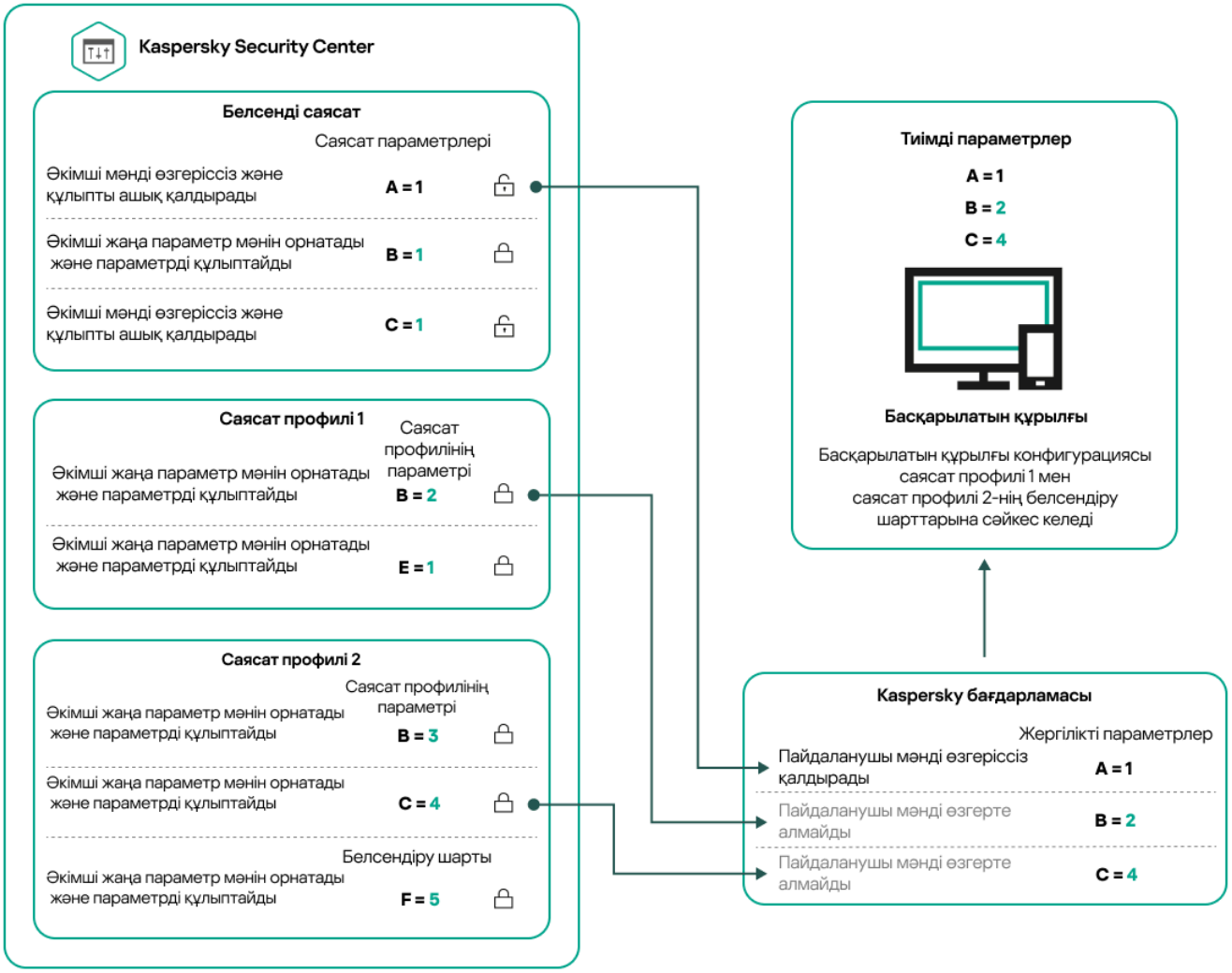
Саясат профильдерінде басымдықты тағайындаудың келесі шарттары бар:

- Саясат профильдерінің тізіміндегі профильдің орны оның басымдылығын білдіреді. Саясат профилінің басымдылығын өзгертуге болады. Тізімдегі ең жоғары жайғасым ең жоғары басымдықты білдіреді (төмендегі суретті қараңыз).



Саясат профилі басымдығын анықтау

- Саясат профильдерін белсендіру шарттары бір-біріне тәуелді емес. Бір уақытта бірнеше саясат профильдерін белсендіруге болады. Егер бірнеше саясат профильдері бірдей параметрге әсер етсе, құрылғы ең жоғары басымдығы бар саясат профиліндегі параметр мәнін пайдаланады (төмендегі суретті қараңыз).



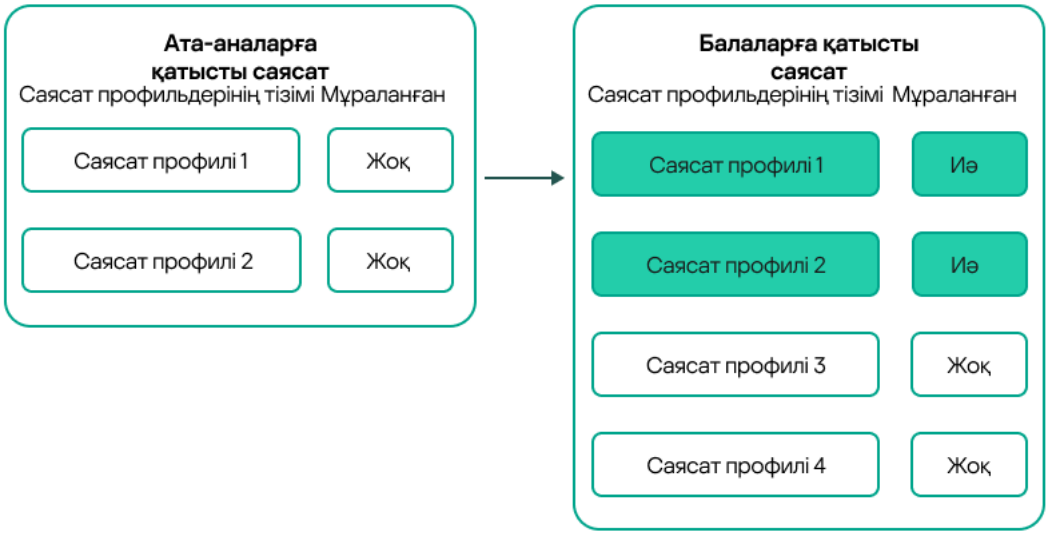
Басқарылатын құрылғының конфигурациясы бірнеше саясат профильдерін белсендіру шарттарына сәйкес келеді

Иелену иерархиясындағы саясат профильдері

Иерархияның әртүрлі деңгейлерінің саясаттарындағы саясат профильдері келесі шарттарға сәйкес келеді:

- Төменгі деңгейдегі саясат аса жоғары деңгейдегі саясаттан саясат профильдерін алады. Жоғары деңгейдегі саясаттан иеленген саясат профилі бастапқы саясат профилінің деңгейіне қарағанда жоғары басымдыққа ие болады.

- Сіз иеленген саясат профилінің басымдылығын өзгерте алмайсыз (төмендегі суретті қараңыз).

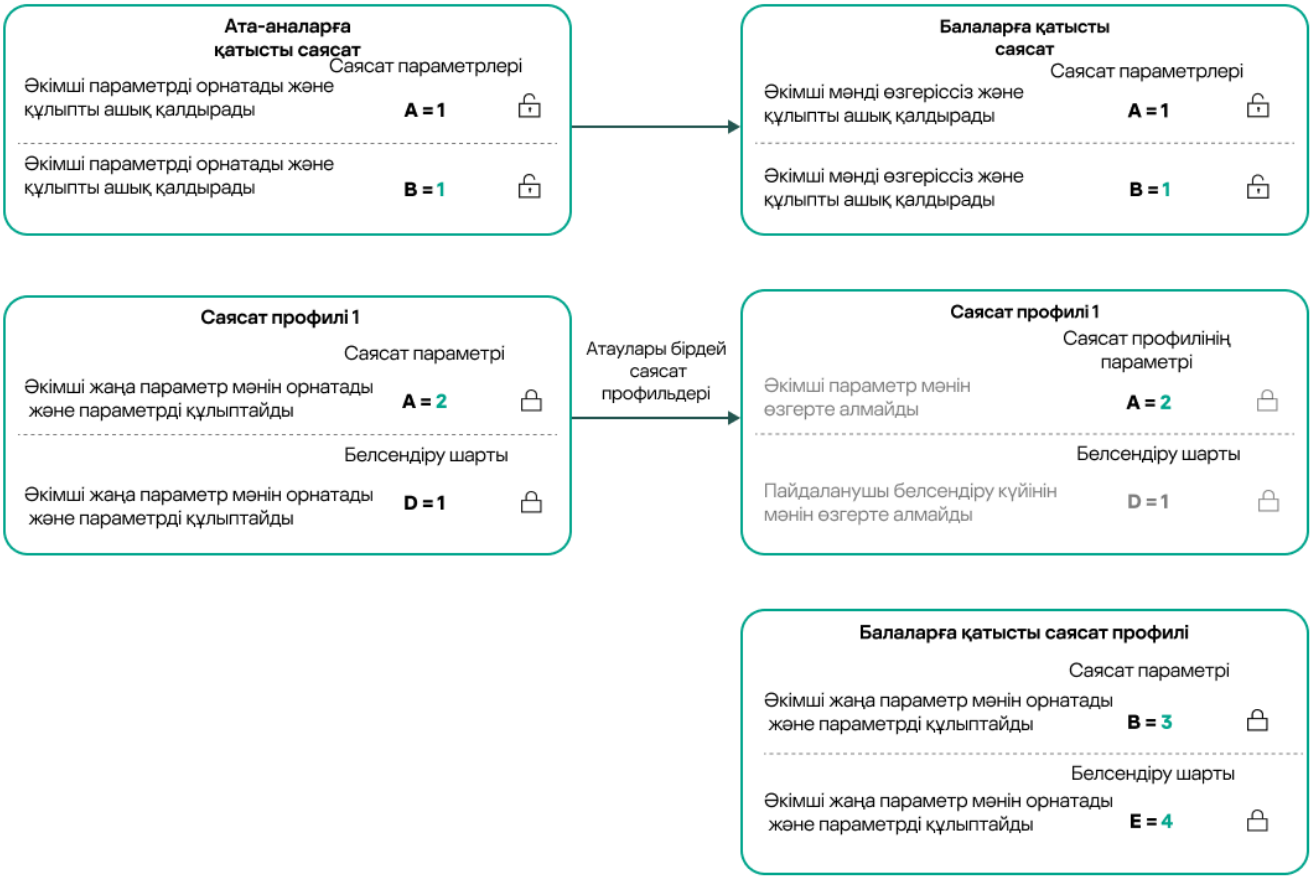


Саясат профильдерінің параметрлерін иелену

Атауы бірдей саясат профильдері

Егер иерархияның әртүрлі деңгейлерінде атаулары бірдей екі саясат болса, бұл саясаттар келесі ережелерге сәйкес жұмыс істейді:

- Аса жоғары деңгейлі саясат профилі үшін құлыпталған параметрлер мен профильді белсендіру шарты ең төменгі деңгейдегі саясат профилі үшін профильді белсендіру параметрлері мен шарттарын өзгертеді (төмендегі суретті қараңыз).



Еншілес профиль тектік саясат профилінен параметрлердің мәндерін алады

- Аса жоғары деңгейлі саясат профилі үшін құлпы ашылған параметрлер мен профильді белсендіру шарты ең төменгі деңгейдегі саясат профилі үшін профильді белсендіру параметрлері мен шарттарын өзгертеді.

Басқарылатын құрылғының параметрлері қалай іске асырылады

Басқарылатын құрылғыда тиімді параметрлердің қолданылуын келесідей сипаттауға болады:

- Барлық құлыпталмаған параметрлердің мәндері саясаттан алынады.
- Содан кейін, олар басқарылатын бағдарлама параметрлерінің мәндерімен қайта жазылады.
- Әрі қарай, қолданыстағы саясаттан бұғатталған параметр мәндері қолданылады. Құлыпталған параметрлердің мәндері құлпы ашылған қолданыстағы параметрлердің мәндерін өзгертеді.

Саясатты басқару

Бұл бөлім саясатты басқаруды сипаттайды және саясат тізімін қарау, саясатты жасау, саясатты өзгерту, саясатты көшіру, саясатты жылжыту, мәжбүрлеп синхрондау, саясатты тарату күйінің диаграммасын қарау және саясатты жою туралы ақпарат береді.

Саясаттар тізімін қарап шығу

Басқару серверінде немесе кез келген басқару тобында жасалған саясаттардың тізімін көре аласыз.

Саясаттар тізімін қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Басқару топтары тізімінен саясат тізімін қарап шыққыңыз келетін басқару тобын таңдаңыз.

Саясаттар кесте түрінде көрсетіледі. Саясаттар болмаса, бос кесте көрсетіледі. Сіз кестенің бағандарын көрсете немесе жасыра аласыз, олардың ретін өзгерте аласыз, тек сіз көрсеткен мәнді қамтитын жолдарды көре аласыз немесе іздеуді қолдана аласыз.

Саясатты жасау

Сіз саясаттар жасай аласыз; қолданыстағы саясаттарды өзгертуге немесе жоюға да болады.

Саясат жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Саясат жасау қажет басқару тобын таңдаңыз:
   - Түбірлік топ үшін.

     Бұл жағдайда келесі қадамға өтуге болады.
   - Ішкі топ үшін:

     a. Терезенің жоғарғы жағындағы ағымдағы жол сілтемесіне өтіңіз.

     b. Ашылған тақтада қажетті ішкі топтың аты бар сілтемеге өтіңіз.

     Ағымдағы жол таңдалған ішкі топты көрсету үшін өзгереді.
3. **Қосу** түймесін басыңыз.

   Бағдарламаны таңдаңыз терезесі ашылады.
4. Саясат жасауды қажет ететін бағдарламаны таңдаңыз.

5. **Келесі** түймесін басыңыз.

   Жалпы қойыншасында жаңа саясат параметрлері терезесі ашылады.

6. Қаласаңыз, әдепкі бойынша белгіленген келесі саясат параметрерін өзгерте аласыз: атауы, күйі және иелену.

7. **Бағдарлама параметрлері** қойыншасын таңдаңыз.

   Не болмаса, шығу үшін **Сақтау** түймесін басыңыз. Саясат саясаттар тізіміне пайда болып, сіз оның сипаттарын кейінірек өзгерте аласыз.

8. **Бағдарлама параметрлері** қойындысының сол жақ панелінде сізге қажетті санатты таңдап, оң жақтағы нәтижелер панелінде саясат параметрлерін өзгертіңіз. Сіз әрбір бөлімдегі саясат параметрлерін өзгерте аласыз.

   Параметрлер жиынтығы, сіз саясат жасап жатқан бағдарламаға байланысты. Толығырақ ақпарат келесі дереккөздерде келтірілген:

   - Басқару серверін конфигурациялау
   - Желілік агент саясатының параметрлері
   - Kaspersky Endpoint Security for Windows құжаттамасы

   Басқа қауіпсіздік бағдарламаларының параметрлері туралы толығырақ білу үшін тиісті бағдарламаның құжаттамасын қараңыз.

   Өзгерістерді болдырмау үшін **Бас тарту** түймесін басуға болады.

9. Саясат өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Нәтижесінде, қосылған саясат саясаттар тізімінде көрсетіледі.

Саясатты өзгерту

Саясатты өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

2. Өзгертуді қажет ететін саясатты таңдаңыз.

   Саясат сипаттары терезесі ашылады.

3. Сіз саясатты жасайтын жалпы параметрлер мен бағдарлама параметрлерін көрсетіңіз. Толығырақ ақпарат келесі дереккөздерде келтірілген:

   - Басқару серверін конфигурациялау
   - Желілік агент саясатының параметрлері
   - Kaspersky Endpoint Security for Windows құжаттамасы

Басқа қауіпсіздік бағдарламаларының параметрлері туралы толығырақ білу үшін осы бағдарламалардың құжаттамасын қараңыз.

4. **Сақтау** түймесін басыңыз.

Саясат өзгерістері саясаттың сипаттарында сақталып, **Тексерістер журналы** бөлімінде көрсетіледі.

Саясаттардың жалпы параметрлері

Жалпы

Жалпы қойыншасында саясаттың күйін өзгертуге және саясат параметрлерін иеленуді конфигурациялауға болады:

- **Саясаттың күйі** блогында саясаттың әрекет ету ауқымы нұсқаларының біреуін таңдауға болады:
  - **Белсенді**

    Осы нұсқа таңдалған болса, саясат белсенді болады.

    Әдепкі бойынша, осы нұсқа таңдалған.
  - **Кеңседен тыс**

    Егер бұл нұсқа таңдалса, құрылғы ұйым желісінен шыққан кезде саясат күшіне енеді.
  - **Белсенді емес**

    Егер бұл нұсқа таңдалса, саясат белсенді болмайды, бірақ **Саясат** қалтасында сақталады. Қажет болса, оны белсенді етуге болады.
- **Параметрлерді иелену** блогында саясатты иелену параметрлерін конфигурациялауға болады:
  - **Параметрлерді негізгі саясаттан иелену**

    Параметр қосулы болса, саясат параметрлері мәндері иерархияның жоғарғы деңгейіндегі топқа арналған саясаттан иеленеді және өзгерту үшін қолжетімді емес.

    Әдепкі бойынша, параметр қосулы.
  - **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену**

    Егер параметр қосылса, саясатқа өзгертулер қолданылғаннан кейін келесі қадамдар орындалады:
    - саясат параметрлерінің мәндері салынған басқару топтарының саясаты – еншілес саясаттарға қатысты қолданылады;
    - Әрбір еншілес саясат сипаттары терезесінің **Жалпы** бөлімінің **Параметрлерді иелену** блогында **Параметрлерді негізгі саясаттан иелену** параметрі автоматты түрде қосылады.

    Параметр қосулы болған кезде, еншілес саясат параметрлерінің мәндерін өзгерту қолжетімді емес.

    Әдепкі бойынша, параметр өшірулі.

Оқиғаларды конфигурациялау

Оқиғаларды конфигурациялау қойыншасында оқиғаларды тіркеуді және оқиғалар туралы хабарлауды конфигурациялауға болады. Оқиғалар қойыншалардағы маңыздылық деңгейлері бойынша бөлінген:

- **Критикалық**

  Критикалық бөлімі Желілік агент саясатының сипаттарында көрсетілмейді.

- **Функционалдық ақау**
- **Ескерту**
- **Ақпараттық**

Оқиғалар тізіміндегі әрбір бөлімде оқиғалардың атаулары және әдепкі бойынша Басқару серверінде оқиғаларды сақтау уақыты (күндерде) көрсетіледі. Оқиға түрін басу арқылы сіз келесі параметрлерді көрсете аласыз:

- **Оқиғаларды тіркеу**

  Сіз оқиғаларды сақтау күндерінің санын көрсете аласыз және оқиғаларды қайда сақтау керектігін таңдай аласыз:

  - **Syslog протоколы арқылы SIEM жүйесіне экспорттау**
  - **Құрылғыдағы ОЖ оқиғалар журналында сақтау**
  - **Басқару серверіндегі ОЖ оқиғалар журналында сақтау**

- **Оқиға хабарландырулары**

  Оқиға хабарландырулары тәсілін таңдауға болады:

  - **Электрондық пошта арқылы хабарлау**
  - **SMS арқылы хабарлау**
  - **Орындалатын файлды немесе сценарийді іске қосып хабарлау**
  - **SNMP арқылы хабарлау**

  Әдепкі бойынша, Басқару сервері сипаттарының қойыншасында көрсетілген хабарландыру параметрлері қолданылады (мысалы, алушының мекенжайы). Қаласаңыз, бұл параметрлерді **Электрондық пошта**, **SMS** және **Іске қосылатын орындалатын файл** қойыншаларында өзгертіңіз.

Тексерістер журналы

Тексерістер журналы қойыншасында сіз саясатты тексеру тізімін және кері қайтарылған өзгерістерді көре аласыз.

Саясатты иелену параметрін қосу және өшіру

Саясатта иелену параметрін қосу немесе өшіру үшін:

1. Қажетті саясатты ашыңыз.
2. **Жалпы** қойыншасын ашыңыз.
3. Саясатты иеленуді қосыңыз немесе өшіріңіз:
   - Егер еншілес топта **Параметрлерді негізгі саясаттан иелену** параметрі қосылған болса және тектік саясаттағы кейбір параметрлер бұғатталса, онда сіз осы саясат параметрлерін еншілес топ үшін өзгерте алмайсыз.
   - Егер еншілес саясатта **Параметрлерді негізгі саясаттан иелену** параметрі өшірулі болса, онда сіз тектік саясатта кейбір параметрлер "бұғатталған" болса да, еншілес саясаттағы барлық параметрлерді өзгерте аласыз.
   - Тектік топта **Еншілес саясаттардағы параметрлерді мәжбүрлеп иелену** параметрі қосулы болса, әрбір еншілес саясат үшін **Параметрлерді негізгі саясаттан иелену** параметрі де қосылады. Бұл жағдайда, сіз осы параметрді еншілес саясат үшін өшіре алмайсыз. Негізгі саясатта бұғатталған барлық параметрлер еншілес топтарда мәжбүрлеп иеленеді және сіз бұл параметрлерді еншілес топтарда өзгерте алмайсыз.
4. Өзгерістерді сақтау үшін **Сақтау** түймесін басыңыз немесе өзгерістерді қабылдамау үшін **Бас тарту** түймесін басыңыз.

Әдепкі бойынша, **Параметрлерді негізгі саясаттан иелену** параметрі жаңа саясат үшін қосулы.

Егер саясатта профильдер болса, барлық еншілес саясаттар осы профильдерді иеленеді.

Саясатты көшіру

Сіз саясатты бір басқару тобынан екіншісіне көшіре аласыз.

Саясаты басқа басқару тобына көшіру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Жалаушаны, көшірілетін саясатқа (немесе саясаттарға) қарама-қарсы қойыңыз.
3. **Көшіру** түймесін басыңыз.

   Экранның оң жағында басқару топтарының ағашы көрсетіледі.
4. Ағашта мақсатты топты, яғни саясатты (немесе саясаттарды) көшіргіңіз келетін топты таңдаңыз.
5. Экранның астындағы **Көшіру** түймесін басыңыз.
6. Операцияны растау үшін **OK** түймесін басыңыз.

Саясат (саясаттар) және оның барлық профильдері мақсатты басқару тобына көшіріледі. Мақсатты топтағы әрбір көшірілген саясат **Белсенді емес** күйін қабылдайды. Саясаттың күйін кез келген уақытта **Белсенді** деп өзгерте аласыз.

Егер саясаттың мақсатты тобында көшірілетін саясаттың атына сәйкес келетін саясат болса, көшірілген саясаттың атына түрдің жалғауы қосылады (<келесі реттік нөмір>), мысалы: (1).

Саясатты жылжыту

Сіз саясаттарды бір басқару тобынан екіншісіне жылжыта аласыз. Мысалы, сіз бір басқару тобын жойғыңыз келеді, бірақ оның саясаттарын басқа басқару тобы үшін қолданғыңыз келеді. Бұл жағдайда, ескі басқару тобын жою алдында саясатты ескі басқару тобынан жаңасына жылжыту қажет болуы мүмкін.

Саясатты басқа басқару тобына ауыстырған кезде, саясаттың түзету тарихы жойылады. **Тексерістер журналы** қойындысында тек соңғы өзгеріс туралы ақпарат көрсетіледі.

Саясатты басқа басқару тобына жылжыту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Жалаушаны, жылжытылатын саясатқа (немесе саясаттарға) қарама-қарсы қойыңыз.
3. **Жылжыту** түймесін басыңыз.

   Экранның оң жағында басқару топтарының ағашы көрсетіледі.
4. Ағашта мақсатты басқару тобын, яғни саясатты (немесе саясаттарды) жылжытқыңыз келетін топты таңдаңыз.
5. Экранның астындағы **Жылжыту** түймесін басыңыз.
6. Операцияны растау үшін **ОК** түймесін басыңыз.

Егер саясат дереккөз тобынан иеленген болмаса, ол барлық саясат профильдері бар мақсатты топқа жылжытылады. Мақсатты басқару тобындағы саясаттың күйі **Белсенді емес** болады. Саясаттың күйін кез келген уақытта **Белсенді** деп өзгерте аласыз.

Саясат дереккөз тобынан иеленген болса, ол дереккөз тобында қала береді. Саясат мақсатты топқа барлық профильдерімен бірге көшірілген. Мақсатты басқару тобындағы саясаттың күйі **Белсенді емес** болады. Саясаттың күйін кез келген уақытта **Белсенді** деп өзгерте аласыз.

Егер саясаттың мақсатты тобында көшірілетін саясаттың атына сәйкес келетін саясат болса, көшірілген саясаттың атына түрдің жалғауы қосылады (<келесі реттік нөмір>), мысалы: (1).

Саясатты экспорттау

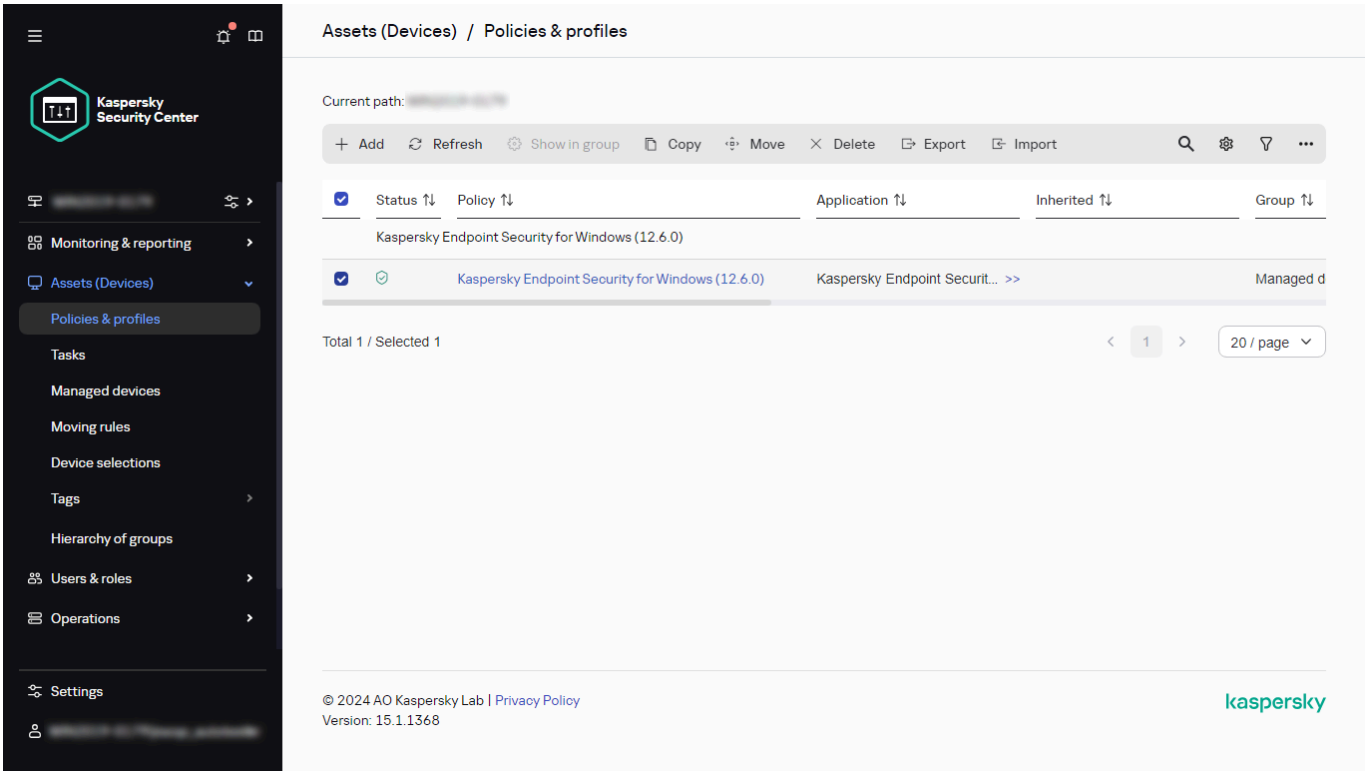
Kaspersky Security Center бағдарламасы саясатты, оның параметрлерін және саясат профильдерін KLP файлына сақтауға мүмкіндік береді. Сақталған саясатты Kaspersky Security Center Windows, сондай-ақ Kaspersky Security Center Linux жүйелерінде импорттау үшін KLP файлын пайдалануға болады.

Саясатты экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

2. Экспорттағыңыз келетін саясаттың жанына жалаушаны қойыңыз.

   Бір уақытта бірнеше саясатты экспорттауға болмайды. Егер сіз бірден артық саясатты таңдасаңыз, **Экспорттау** түймесі белсенді емес болмайды.



3. **Экспорттау** түймесін басыңыз.

4. Ашылған **Басқаша сақтау** терезесінде саясат файлының атауы мен жолын көрсетіңіз. **Сақтау** түймесін басыңыз.

   Басқаша сақтау терезесі Google Chrome, Microsoft Edge немесе Opera қолдансаңыз ғана көрсетіледі. Басқа браузерді қолданып жатсаңыз, саясат файлы автоматты түрде **Жүктеп алулар** қалтасына сақталады.

Саясатты импорттау

Kaspersky Security Center бағдарламасы саясатты KLP файлынан импорттауға мүмкіндік береді. KLP файлында экспортталған саясат, оның параметрлері және саясат профильдері бар.

Саясатты импорттау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

2. **Импорттау** түймесін басыңыз.

3. Импорттағыңыз келетін саясат файлын таңдау үшін **Шолу** түймесін басыңыз.

4. Ашылған терезеде KLP саясаты файлына апаратын жолды көрсетіңіз және **Ашу** түймесін басыңыз. Назар аударыңыз, сіз тек бір саясатын файлын ғана таңдай аласыз.

   Саясатты өңдеу басталады.

5. Саясатты өңдеу сәтті аяқталғаннан кейін, саясатты қолданғыңыз келетін басқару тобын таңдаңыз.

6. Саясатты импорттауды аяқтау үшін **Аяқтау** түймесін басыңыз.

Импорт нәтижелері бар хабарландыру пайда болады. Саясатты импорттау сәтті орындалса, сіз саясат сипаттарын қарап шығу үшін **Мәліметтер** сілтемесінен өте аласыз.

Импорт сәтті орындалғаннан кейін, саясат саясаттар тізімінде көрсетіледі. Сондай-ақ, саясат параметрлері мен профильдері импортталады. Экспортта таңдалған саясаттың күйіне қарамастан, импортталатын саясат белсенді емес. Саясат сипаттарындағы саясаттың күйін өзгертуге болады.

Импортталған жаңа саясаттың атауы бұрыннан бар саясаттың атауымен бірдей болса, импортталған саясаттың атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Саясатты қолдану күйінің диаграммасын қарау

Kaspersky Security Center бағдарламасында диаграммадағы әрбір құрылғыда саясатты қолдану күйін көруге болады.

Әр құрылғыда саясатты қолдану күйін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

2. Құрылғыдағы қолдану күйін көргіңіз келетін саясат атауының жанына жалаушаны қойыңыз.

3. Пайда болған мәзірден **Тарату** тармағын таңдаңыз.

   <саясат атауы> тарату нәтижесі терезесі ашылады.

4. Ашылған **<саясат атауы> тарату нәтижесі** терезесінде **Күйдің сипаттамасы** көрсетіледі.

Саясатты қолдану нәтижелері тізімінде көрсетілген нәтижелер санын өзгертуге болады. Құрылғылардың ең көп саны: 100,000.

Саясатты қолдану нәтижелерімен бірге тізімде көрсетілген құрылғылардың санын өзгерту үшін:

1. Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Интерфейс опциялары** тармағын таңдаңыз.

2. **Саясаттың тарату нәтижелерінде көрсетілетін құрылғылардың шегінде** құрылғылардың санын (100 000-ға дейін) енгізіңіз.

   Құрылғылардың әдепкі бойынша саны: 5000.

3. **Сақтау** түймесін басыңыз.

   Параметрлер сақталған және қолданылған.

Саясатты жою

Саясатты қажет болмаған кезде жоя аласыз. Таңдалған басқару тобында иеленбеген саясатты ғана жоюға болады. Егер саясат иеленген болса, оны тек ол жасалған басқару тобында жоюға болады.

Саясатты жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Жалаушаны, жойғыңыз келетін саясат атының жанына қойып, **Жою** түймесін басыңыз.

   Иеленген саясатты таңдаған болсаңыз, **Жою** түймесі белсенді емес (сұр) болады.
3. Операцияны растау үшін **ОК** түймесін басыңыз.

Саясат және оның саясат профильдерінің барлығы жойылған.

Саясат профильдерін басқару

Бұл бөлім саясат профильдерін басқаруды сипаттайды және саясат профильдерін қарау, саясат профилінің басымдылығын өзгерту, саясат профилін жасау, саясат профилін өзгерту, саясат профилін көшіру, саясат профилін белсендіру ережесін жасау және саясат профилін жою туралы ақпарат береді.

Саясат профильдерін қарау

Саясат профильдерін қарау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Профильдерін қарау қажет саясатты таңдаңыз.

   Жалпы қойыншасында саясат сипаттары терезесі ашылады.
3. **Саясат профильдері** қойыншасын ашыңыз.

Саясат профильдері кесте түрінде көрсетіледі. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.

Саясат профилі басымдығын өзгерту

Саясат профилі басымдығын өзгерту үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.
2. **Саясат профильдері** қойыншасында, басымдығын өзгерту керек болған саясат профилінің жанында жалаушаны қойыңыз.

3. Саясат профилін **Басымдық беру** немесе **Басымдығын жою** түймелерінің көмегімен тізімдегі жаңа жайғасымға қойыңыз.

   Тізімдегі саясат профилі неғұрлым жоғары болса, оның басымдығы да соғұрлым жоғары болады.

4. **Сақтау** түймесін басыңыз.

Таңдалған саясат профилі басымдығы өзгертілген және қолданылған.

Саясат профилін жасау

Саясат профилін жасау үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.

2. **Қосу** түймесін басыңыз.

3. Қажет болса, әдепкі бойынша белгіленген саясат профилінің иелену параметрлері мен атауын өзгертіңіз.

4. **Бағдарлама параметрлері** қойыншасын таңдаңыз.

   Шығу үшін **Сақтау** түймесін басуға да болады. Құрылған саясат профилі саясат профильдерінің тізімінде көрсетіліп, сіз оның сипаттарын кейінірек өзгерте аласыз.

5. **Бағдарлама параметрлері** қойыншасының сол жағында, сізге қажетті бөлімді таңдап, нәтижелер тақтасында саясат профилі параметрлерін өзгертіңіз. Сіз әрбір бөлімдегі саясат профилі параметрлерін өзгерте аласыз.

   Өзгерістерді болдырмау үшін **Бас тарту** түймесін басуға болады.

6. Профиль өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Саясат профилі саясат профильдері тізімінде көрсетіледі.

Саясат профилін өзгерту

Профильді өзгерту тек Kaspersky Endpoint Security for Windows саясаттары үшін ғана қолжетімді.

Саясат профилін өзгерту үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. **Саясат профильдері** қойыншасында өзгерткіңіз келетін саясат профилін нұқыңыз.

   Нәтижесінде, саясат профилі сипаттары терезесі ашылады.

3. Сипаттар терезесінде профиль параметрлерін конфигурациялаңыз:

   - Қажет болса, **Жалпы** қойыншасында саясат профилінің атын өзгертіңіз және профильді қосыңыз немесе өшіріңіз.
   - Саясатын профилін белсендіру ережелерін өзгертіңіз.
   - Қалған параметрлерді өзгертіңіз.

   Қауіпсіздік бағдарламаларының параметрлері туралы толығырақ білу үшін тиісті бағдарламаның құжаттамасын қараңыз.

4. **Сақтау** түймесін басыңыз.

Өзгертілген параметрлер құрылғыны Басқару серверімен синхрондағаннан кейін (саясат профилі белсенді болса) немесе белсендіру ережесін орындағаннан кейін (саясат профилі белсенді болмаса) әрекет ете бастайды.

Саясат профилін көшіру

Саясат профилін ағымдағы саясатқа немесе басқа саясатқа көшіруге болады, мысалы, әртүрлі саясаттар үшін бірдей саясат профильдеріне ие болғыңыз келсе. Сондай-ақ, егер сіз параметрлердің аз санымен ерекшеленетін екі немесе одан да көп саясат профиліне ие болғыңыз келсе, көшіруді пайдалана аласыз.

Саясат профилін көшіру үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады. Саясатта саясат профильдері болмаса, бос кесте көрсетіледі.

2. **Саясат профильдері** қойыншасында көшіру қажет болған профильді таңдаңыз.

3. **Көшіру** түймесін басыңыз.

4. Ашылған терезеде саясат профилін көшіру қажет болған саясатты таңдаңыз.

   Саясат профилін сол саясатқа немесе сіз таңдаған саясатқа көшіруге болады.

5. **Көшіру** түймесін басыңыз.

Саясат профилі сіз таңдаған саясатқа көшірілді. Жаңа көшірілген саясат профилі ең төменгі басымдыққа ие. Сіз саясат профилін сол саясатқа көшірген болсаңыз, осындай профильдің атауына түрдің жалғауы (<реттік нөмір>) қосылады, мысалы: (1), (2).

Кейінірек профиль параметрлерін, соның ішінде оның атауын және басымдығын өзгертуге болады; бұл жағдайда бастапқы саясат профилі өзгертілмейді.

Саясатын профилін белсендіру ережесін жасау

Саясатын профилін белсендіру ережесін жасау үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. **Саясат профильдері** қойыншасында белсендіру ережесін жасауды қажет ететін саясат профилін басыңыз.

   Саясат профильдері тізімі бос болса, саясат профилін жасай аласыз.

3. **Белсендіру ережелері** қойыншасында **Қосу** түймесін басыңыз.

   Саясат профилін белсендіру ережелері бар терезе ашылады.

4. Белсендіру ережесінің атын көрсетіңіз.

5. Жасалғалы жатқан саясат профилін белсендіруге әсер етуі тиісті шарттарға қарама-қарсы жалаушалар қойыңыз:

   - **Саясат профилін белсендірудің жалпы ережелері**

     Құрылғының автономды режимі күйіне, құрылғыны Басқару серверіне қосу ережелеріне және құрылғыға тағайындалған тегтерге байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

     Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

     - **Құрылғының күйі**

       Құрылғының желіде болу шартын анықтайды:

       - **Онлайн** – құрылғы желіде орналасқан, Басқару сервері қолжетімді.
       - **Офлайн** – құрылғы сыртқы желіде орналасқан, яғни Басқару сервері қолжетімді емес.
       - **Қолданылмайды** – өлшемшарт қолданылмайды.

     - **Бұл құрылғыда Басқару сервері байланысының ережесі белсенді**

       Саясат профилін белсендіру үшін шартты таңдаңыз (бұл ереже орындалса да, орындалмаса да) және ереже атауын таңдаңыз.

       Ереже, шарттарын орындау немесе орындамау кезінде саясат профилі белсендірілетін Басқару серверіне қосылуға арналған құрылғының желілік орнымен анықталады.

       Басқару серверіне қосылу үшін құрылғылардың желілік орнының сипаттамасын Желілік агентті ауыстырып қосу ережесінде жасауға немесе конфигурациялауға болады.

   - **Арнайы құрылғы иесіне арналған ережелер**

     Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

     - **Құрылғының иесі**

       Құрылғының иесі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

       - құрылғы көрсетілген иеленушіге тисілі ("=" белгісі);
       - құрылғы көрсетілген иеленушіге тисілі емес ("#" белгісі).

         Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Параметр қосылған кезде, құрылғы иесін көрсетуіңізге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Құрылғы иесі ішкі қауіпсіздік тобына кіреді**

  Kaspersky Security Center ішкі қауіпсіздік тобындағы құрылғы иесінің мүшелігі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

  - құрылғының иесі көрсетілген қауіпсіздік тобының мүшесі ("=" белгісі);
  - құрылғының иесі көрсетілген қауіпсіздік тобының мүшесі емес ("#" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Сіз Kaspersky Security Center қауіпсіздік тобын көрсете аласыз. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Жабдық сипаттамалары ережелері**

  Жадтың көлеміне және құрылғының логикалық процессорларының санына байланысты құрылғыдағы саясатты белсендіру шартын конфигурациялау үшін жалаушаны қойыңыз.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Жедел жадтың көлемі, МБ түрінде**

    Құрылғының жедел жад көлемі бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

    - құрылғының жедел жады көлемі көрсетілген мәннен аз ("<" белгісі);
    - құрылғының жедел жады көлемі көрсетілген мәннен артық (">" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Құрылғының жедел жадының көлемін көрсетуге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

  - **Логикалық процессорлардың саны**

    Құрылғының логикалық процессорлардың саны бойынша құрылғыдағы профильді белсендіру ережесін конфигурациялау және қосу үшін параметрді қосыңыз. Жалауша астындағы ашылмалы тізімнен профильді белсендіру өлшемшартын таңдауға болады:

    - құрылғының логикалық процессорларының саны көрсетілген мәннен аз немесе оған тең ("<" белгісі);
    - құрылғының логикалық процессорларының саны көрсетілген мәннен артық немесе оған тең (">" белгісі).

    Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады. Құрылғының логикалық процессорларының санын көрсетуіңізге болады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

- **Рөлді тағайындау ережелері**

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  Құрылғы иесінің арнайы рөлі бойынша саясат профилін белсендіру

  Құрылғы иесінің белгілі бір рөлінің болуына байланысты, құрылғыда саясат профилін белсендіру ережесін конфигурациялау және қосу үшін осы параметрді қосыңыз. Қолданыстағы рөлдер тізімінен рөлді қолмен қосыңыз.

Параметр қосулы болса, құрылғыдағы профильді белсендіру конфигурацияланған өлшемшартқа сәйкес орындалады.

- **Тегті қолдану ережелері**

  Құрылғыға тағайындалған тегтерге байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз. Саясат профилін таңдалған тегтері бар немесе жоқ құрылғыларда белсендіруге болады.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Тег**

    Тегтер тізімінде қажетті тегтерге жалаушалар қою арқылы құрылғыларды саясат профиліне қосу ережесін белгілеңіз.

    Тізімге жаңа тегтерді қосу үшін оларды тізімнің үстіндегі өріске енгізіп, **Қосу** түймесін басуыңызға болады.

    Саясат профиліне, сипаттамасында барлық таңдалған тегтері бар құрылғылар қосылады. Жалаушалар алынып тасталса, өлшемшарт қолданылмайды. Әдепкі бойынша, жалаушалар алынып тасталған.

  - **Көрсетілген тегтерсіз құрылғыларға қолдану**

    Тег таңдауын терістету қажет болса, параметрді қосыңыз.

    Параметр қосулы болса, онда саясат профиліне, сипаттамасында таңдалған тегтері жоқ құрылғылар қосылады. Бұл параметр өшірулі болса, өлшемшарт қолданылмайды.

    Әдепкі бойынша, параметр өшірулі.

- **Active Directory қызметін пайдалану ережелері**

  Құрылғының Active Directory бөлімшесінде орналасуына немесе құрылғының не оның иесінің Active Directory қауіпсіздік тобына мүше болуына байланысты құрылғыдағы саясат профилін белсендіру ережелерін конфигурациялау үшін жалаушаны қойыңыз.

  Бұл параметр үшін келесі қадамда мынаны көрсетіңіз:

  - **Құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі**

    Параметр қосулы болса, онда саясат профилі, иесі аталған қауіпсіздік тобының мүшесі болып табылатын құрылғыда іске қосылады. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

  - **Құрылғының Active Directory қауіпсіздік тобындағы мүшелігі**

    Параметр қосулы болса, құрылғыда саясат профилі белсендіріледі. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды. Әдепкі бойынша, параметр өшірулі.

  - **Active Directory бөлімшесіне құрылғыны орналастыру**

    Параметр қосулы болса, саясат профилі көрсетілген Active Directory бөлімшесіне кіретін құрылғыда белсендіріледі. Бұл параметр өшірулі болса, профильді белсендіру өлшемшарты қолданылмайды.

    Әдепкі бойынша, параметр өшірулі.

Шебер терезелерінің кейінгі саны осы қадамдағы параметрлерді таңдауға байланысты. Саясат профилін белсендіру ережелерін кейінірек өзгертуге болады.

6. Конфигурацияланған параметрлер тізімін тексеріңіз. Тізімі дұрыс болса, **Жасау** түймесін басыңыз.

Нәтижесінде, профиль сақталады. Белсендіру ережелері орындалған кезде профиль құрылғыда белсендіріледі.

Профиль үшін жасалған саясат профилін белсендіру ережелері **Белсендіру ережелері** қойыншасындағы саясат профилінің сипаттарында көрсетіледі. Саясат профилін белсендіру ережесін өзгертуге немесе жоюға болады.

Бірнеше белсендіру ережесі бір уақытта орындалуы мүмкін.

Саясат профилін жою

Саясат профилін жою үшін:

1. Таңдалған саясат профильдері тізіміне өтіңіз.

   Саясат профильдері тізімі ашылады.

2. **Саясат профильдері** бетінде, жойғыңыз келетін саясат профилінің жанында жалауша қойып, **Жою** түймесін басыңыз.

3. Пайда болған терезеде **Жою** түймесін тағы да басыңыз.

Саясат профилі жойылды. Егер саясатты аса төменгі деңгейдегі топ иеленсе, саясат профилі осы топта қала береді, бірақ осы топтың саясат профиліне айналады. Бұл, төменгі деңгейдегі топтардың құрылғыларына орнатылған басқарылатын бағдарламалардың параметрлерінде өзгерістерді азайтуға мүмкіндік береді.

Деректерді шифрлау және қорғау

Деректерді шифрлау, портативті құрылғыны немесе қатты дискіні ұрлаған/жоғалтқан жағдайда немесе деректерге авторизацияланбаған пайдаланушылар мен бағдарламалар қатынасқан жағдайда ақпараттың абайсызда ағып кету қаупін азайтады.

Шифрлауды келесі Kaspersky бағдарламалары қолдайды:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Пайдаланушы интерфейсінің параметрлері арқылы шифрлауды басқаруға қатысты кейбір интерфейс элементтерін көрсетуге немесе жасыруға болады.

VDI жүйесінде шифрлауды қосуға кеңес бермейміз.

Kaspersky Endpoint Security for Windows бағдарламасында деректерді шифрлау

Шифрлаудың келесі түрлерін басқаруға болады:

- Windows Server операциялық жүйесі жұмыс істейтін құрылғыларда BitLocker дискісін шифрлау;
- Windows for Workstations операциялық жүйесі жұмыс істейтін құрылғыларда Kaspersky дискісін шифрлау.

Kaspersky Endpoint Security for Windows құрамдастарының көмегімен, мысалы, шифрлауды қосуға немесе өшіруге, шифрланған қатты дискілердің тізімін көруге, шифрлау туралы есептерді құруға және көруге болады.

Kaspersky Security Center-де Kaspersky Endpoint Security for Windows саясаттарын конфигурациялай отырып, шифрлауды басқарасыз. Kaspersky Endpoint Security for Windows бағдарламасы белсенді саясатқа сәйкес шифрлауды және шифрсыздауды орындайды. Ережелерді конфигурациялау бойынша толығырақ нұсқаулар және шифрлау ерекшеліктерінің сипаттамасы Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасында берілген.

Kaspersky Endpoint Security for Mac бағдарламасында деректерді шифрлау

macOS операциялық жүйелері бар құрылғыларда FileVault шифрлауын қолдана аласыз. Kaspersky Endpoint Security for Mac бағдарламасымен жұмыс істеу кезінде, сіз осы шифрлауды қоса аласыз немесе өшіре аласыз.

Kaspersky Security Center-де Kaspersky Endpoint Security for Mac саясаттарын конфигурациялай отырып, шифрлауды басқарасыз. Kaspersky Endpoint Security for Mac бағдарламасы белсенді саясатқа сәйкес шифрлауды және шифрсыздауды орындайды. Шифрлау функцияларының егжей-тегжейлі сипаттамасы Kaspersky Endpoint Security for Mac онлайн-анықтамасында келтірілген.

Шифрланған қатты дискілер тізімін қарау

Kaspersky Security Center бағдарламасында сіз шифрланған қатты дискілер туралы және дискілер деңгейінде шифрланған құрылғылар туралы ақпаратты қарай аласыз. Дискіде ақпарат шифрсызданғаннан кейін, диск тізімнен автоматты түрде алынып тасталады.

Шифрланған қатты дискілер тізімін қарау үшін,

Бағдарламаның негізгі терезесінде **Операциялар → Деректерді шифрлау және қорғау → Шифрланған құрылғы** бөліміне өтіңіз.

Бөлім мәзірде болмаса, демек, ол жасырылған. Пайдаланушы интерфейсі конфигурацияларында бөлімді көрсету үшін **Деректерді шифрлау және қорғау опциясын көрсету** параметрін қосыңыз.

Шифрланған қатты дискілер тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады. Бұл үшін **CSV файлына экспорттау** немесе **TXT файлына экспорттау** түймесін басыңыз.

Шифрлау оқиғалары тізімін қарау

Kaspersky Endpoint Security for Windows құрылғыларындағы деректерді шифрлау немесе шифрсыздау тапсырмаларын орындау барысында Kaspersky Security Center бағдарламасына келесі типтегі оқиғалар туралы ақпарат жібереді:

- дискідегі орынның жетіспеушілігіне байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес;
- лицензиямен байланысты мәселелерге байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес;
- қатынасу құқықтарының болмауына байланысты файлды шифрлау немесе шифрсыздау немесе шифрланған мұрағат жасау мүмкін емес;
- бағдарламаға шифрланған файлға қатынасуға тыйым салынған;
- Белгісіз қателер.

Құрылғыларда деректерді шифрлау кезінде туындаған оқиғалар тізімін қарап шығу үшін:

бағдарламаның негізгі терезесінде **Операциялар** → **Деректерді шифрлау және қорғау** → **Шифрлау оқиғалары** бөліміне өтіңіз.

Бөлім мәзірде болмаса, демек, ол жасырылған. Пайдаланушы интерфейсі конфигурацияларында бөлімді көрсету үшін **Деректерді шифрлау және қорғау опциясын көрсету** параметрін қосыңыз.

Шифрланған қатты дискілер тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады. Бұл үшін **CSV файлына экспорттау** немесе **TXT файлына экспорттау** түймесін басыңыз.

Сондай-ақ, әрбір басқарылатын құрылғы үшін шифрлау оқиғалары тізімін қарап шығуға да болады.

Басқарылатын құрылғының шифрлау оқиғаларын қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Басқарылатын құрылғының атын басыңыз.
3. **Жалпы** қойындысында **Қорғаныс** бөліміне өтіңіз.
4. **Деректерді шифрлау қателерін қарап шығу** сілтемесінен өтіңіз.

Шифрлау туралы есептерді қалыптастыру және қарау

Сіз келесі есептерді құрастыра аласыз:

- Басқарылатын құрылғыларды шифрлаудың күйі туралы есеп. Бұл есепте түрлі басқарылатын құрылғылардың деректерін шифрлау туралы мәлімет көрсетілген. Мысалы, есепте конфигурацияланған шифрлау ережелері бар саясат қолданылатын құрылғылардың саны көрсетілген. Сондай-ақ, мысалы, қанша құрылғыны қайта іске қосу керектігін білуге болады. Сондай-ақ, есепте әрбір құрылғы үшін шифрлау технологиясы мен алгоритмі туралы ақпарат қамтылған.

- Жаппай сақтау құрылғыларының шифрлау күйлері туралы есеп беру. Бұл есеп, басқарылатын құрылғыларды шифрлау күйі туралы есепке ұқсас ақпаратты қамтиды, бірақ деректерді тек жаппай сақтау құрылғыларына және алынбалы жетектерге ғана ұсынады.

- Шифрланған құрылғыға қатынасу құқықтары туралы есеп. Бұл есеп шифрланған қатты дискіге қандай пайдаланушы есептік жазбалары кіретінін көрсетеді.

- Файлдарды шифрлау қателері туралы есеп. Есепте құрылғылардағы деректерді шифрлау немесе шифрсыздау тапсырмаларын орындау кезінде пайда болған қателер туралы ақпарат бар.

- Шифрланған файлдарға қатынасты бұғаттау туралы есеп. Есепте бағдарламалардың шифрланған файлдарға қатынасуын бұғаттау туралы ақпарат бар. Бұл есеп, авторизацияланбаған пайдаланушы немесе бағдарлама шифрланған файлдарға немесе қатты дискілерге қатынас алуға әрекеттеніп жатса, пайдалы болады.

Сіз **Бақылау және есеп беру** → **Есептер** бөлімінде кез келген есептемені іске қоса аласыз. Сондай-ақ **Операциялар** → **Деректерді шифрлау және қорғау** бөлімінде келесі шифрлау есептерін жасауға болады:

- Жаппай сақтау құрылғыларының шифрлау күйлері туралы есеп беру

- Шифрланған құрылғыға қатынасу құқықтары туралы есеп

- Файлдарды шифрлау қателері туралы есеп

Деректерді шифрлау және қорғау *бөлімінде шифрлау есептемесін іске қосу үшін:*

1. Интерфейс параметрлерінде **Деректерді шифрлау және қорғау опциясын көрсету** параметрі қосулы екеніне көз жеткізіңіз.

2. Саясат сипаттары терезесінде **Оқиғаларды конфигурациялау** қойыншасына өтіңіз.

3. **Критикалық** бөлімінде **Оқиғаны қосу** түймесін басып, *Файлдарды шифрлау/шифрын шешу ережелерін қолдану қатесі* оқиғасының жанындағы құсбелгіні қойыңыз.

4. **ОК** түймесін басыңыз.

5. Бағдарламаның негізгі терезесінде **Операциялар** → **Деректерді шифрлау және қорғау** бөліміне өтіңіз.

6. Келесі бөлімдердің бірін ашыңыз:

   - **Шифрланған құрылғы** – жаппай сақтау құрылғыларын шифрлау күйі туралы есепті немесе шифрланған құрылғыға қатынасу құқықтары туралы есепті іске қосады.

   - **Шифрлау оқиғалары** – файлдарды шифрлау қателері туралы есепті іске қосады.

7. Іске қосу қажет есептің атауын таңдаңыз.

Есепті іске қосу процесі басталады.

Шифрланған қатты дискіге автономды режимде қатынасу мүмкіндігін ұсыну

Пайдаланушы шифрланған құрылғыға қатынасуды сұрай алады, мысалы, егер Kaspersky Endpoint Security for Windows бағдарламасы басқарылатын құрылғыға орнатылмаған болса. Сұрауды алғаннан кейін сіз қатынасу кілті файлын жасап, оны пайдаланушыға жібере аласыз. Барлық қолдану нұсқалары және толық нұсқаулар Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген.

Шифрланған қатты дискіге автономды режимде қатынасу мүмкіндігін ұсыну үшін:

1. Пайдаланушыдан қатынасты сұрау файлын алыңыз (FDERTC кеңейтімі бар файл). Kaspersky Endpoint Security for Windows бағдарламасында файлды жасау үшін Kaspersky Endpoint Security for Windows онлайн-анықтамасындағы нұсқауларды орындаңыз.

2. Бағдарламаның негізгі терезесінде **Операциялар → Деректерді шифрлау және қорғау → Шифрланған құрылғы** бөліміне өтіңіз.

   Шифрланған қатты дискілер тізімі көрсетіледі.

3. Пайдаланушы қатынас сұрағаң дискіні таңдаңыз.

4. **Құрылғыға офлайн режимде қатынасуға рұқсат беру** түймесін басыңыз.

5. Ашылған терезеде таңдалған дискіні шифрлау үшін пайдаланылған Kaspersky бағдарламасына сәйкес келетін плагинді таңдаңыз.

   Егер қатты диск Kaspersky Security Center Web Console қолдамайтын Kaspersky бағдарламасы арқылы шифрланған болса, онда дискіге автономды режимде қатынас ұсыну үшін Microsoft Management Console (MMC) басқару консоліне негізделген Басқару консолін пайдаланыңыз.

6. Kaspersky Endpoint Security for Windows онлайн-анықтамасында келтірілген нұсқауларды орындаңыз (бөлімнің соңындағы ашылмалы блоктарды қараңыз).

Содан соң, пайдаланушы алынған файлды шифрланған қатты дискіге қатынасу үшін және дискіде сақталатын деректерді оқу үшін пайдалана алады.

Пайдаланушылар және пайдаланушы рөлдері

Бұл бөлімде пайдаланушылармен және пайдаланушы рөлдерімен жасалатын жұмыс сипатталған, сондай-ақ оларды құру және өзгерту, пайдаланушыларға рөлдер мен топтарды тағайындау және саясат профильдерін рөлдермен байланыстыру бойынша нұсқаулар келтірілген.

Пайдаланушы рөлдері туралы

Пайдаланушы рөлі (бұдан әрі *рөл* деп те аталады) – бұл құқықтар мен рұқсаттар жиынтығын қамтитын нысан. Рөл, пайдаланушының құрылғысында орнатылған Kaspersky бағдарламаларының параметрлерімен байланысты болуы мүмкін. Сіз рөлді пайдаланушылар жиынтығына немесе қауіпсіздік топтарының жиынтығына басқару топтары иерархиясының, Басқару серверлерінің кез келген деңгейінде немесе нақты нысандар деңгейінде тағайындай аласыз.

> Егер сіз құрылғыларды виртуалды Басқару серверлерін қамтитын Басқару сервері иерархиясы арқылы басқарсаңыз, пайдаланушы рөлдерін тек физикалық Басқару серверінде жасауға, өзгертуге және жоюға болатынын ескеріңіз. Содан кейін, сіз қосалқы Басқару серверлеріне, соның ішінде виртуалды Серверлерге пайдаланушы рөлдерін тарата аласыз.

Сіз рөлдерді саясат профильдерімен байланыстыра аласыз. Егер пайдаланушыға рөл тағайындалған болса, пайдаланушы қызметтік міндеттерді орындауға қажетті қауіпсіздік параметрлерін алады.

Пайдаланушы рөлі белгіленген басқару тобы пайдаланушыларының құрылғыларымен байланысты болуы мүмкін.

Пайдаланушы рөлі ауқымы

Пайдаланушы рөлі ауқымы – бұл пайдаланушылар мен басқару топтарының тіркесімі. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Рөлдерді пайдаланудың артықшылығы

Рөлдерді пайдаланудың артықшылығы, әрбір басқарылатын құрылғы үшін немесе әрбір пайдаланушы үшін қауіпсіздік параметрлерін бөлек көрсетудің қажеті жоқ. Компаниядағы пайдаланушылар мен құрылғылардың саны көп болуы мүмкін, бірақ әртүрлі қауіпсіздік конфигурацияларын қажет ететін әртүрлі жұмыс функцияларының саны айтарлықтай аз.

Саясат профильдерін қолданудан ерекшеліктері

Саясат профильдері – бұл Kaspersky әр бағдарламасы үшін бөлек құрылған саясаттың сипаттары. Рөл әртүрлі бағдарламалар үшін жасалған көптеген саясат профильдерімен байланысты. Осылайша, рөл – белгілі бір пайдаланушы түріне арналған параметрлерді біріктіру әдісі болып табылады.

Пайдаланушылардың есептік жазбалары мен сеанстарын қарау

Kaspersky Security Center пайдаланушы есептік жазбалары мен есептік жазбалар топтарын басқаруға мүмкіндік береді. Бағдарлама есептік жазбалардың екі түрін қолдайды:

- Ұйым қызметкерлерінің есептік жазбалары. Басқару сервері ұйымның желісінде сауалнама жүргізу кезінде осы пайдаланушылардың есептік жазбалары туралы мәліметтерді алады.
- Ішкі пайдаланушылардың есептік жазбалары. Виртуалды Басқару серверлерімен жұмыс істеу үшін қолданылады. Ішкі пайдаланушы есептік жазбалары тек Kaspersky Security Center ішінде жасалады және пайдаланылады.

Пайдаланушы есептік жазбаларының және сеанстарының тізімін келесі жолдардың бірімен көре аласыз:

- Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіңіз.
- Негізгі мәзірде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** → <құрылғы атауы> сілтемесі бөлімі → **Жалпы** қойындысы → **Жалпы** бөлімі → **Сеанстар** блогына өтіңіз.

  Сеанстар бөлімінде Windows басқаратын құрылғыларда белсенді сеанстары бар пайдаланушылар есептік жазбалары көрсетіледі.

Келесі талаптар орындалса, пайдаланушы есептік жазбалары мен сеанстарының тізімі дұрыс шығады:

- Нұсқасы басқару серверінің нұсқасымен бірдей немесе одан жоғары желілік агент қолданылып жатыр.
- Active Directory сұрауы домен пайдаланушыларының есептік жазбаларын көрсету үшін қосылған.
- Windows басқаратын құрылғыларда **Сервер** қызметі (**LanmanServer**) жұмыс істейді.

Бағдарлама функцияларына қатынасу құқықтарын конфигурациялау. Рөлге негізделген қатынасуды басқару

Kaspersky Security Center бағдарламасы рөлдер негізінде Kaspersky Security Center функцияларына және Kaspersky басқарылатын бағдарламаларының функцияларына қатынасуды қамтамасыз етеді.

Сіз Kaspersky Security Center пайдаланушылары үшін бағдарлама функцияларына қатынасу құқығын келесі тәсілдердің бірімен конфигурациялай аласыз:

- әр пайдаланушының немесе пайдаланушылар тобының құқықтарын жеке-жеке конфигурациялау;
- алдын ала конфигурацияланған құқықтар жиынтығы бар типтік пайдаланушы рөлдерін жасау және пайдаланушыларға олардың қызметтік міндеттеріне қарай рөлдер тағайындау.

Пайдаланушы рөлдерін қолдану пайдаланушының бағдарламаға қатынасу құқығын конфигурациялаудың күнделікті әрекеттерін жеңілдетеді және азайтады. Рөлдегі қатынасу құқықтары пайдаланушылардың типтік тапсырмалары мен қызметтік міндеттеріне сәйкес конфигурацияланады.

Пайдаланушы рөлдеріне олардың мақсатына сәйкес атаулар берілуі мүмкін. Бағдарламада рөлдердің шексіз санын жасай аласыз.

Сіз алдын ала анықталған пайдаланушы рөлдерін бұрыннан конфигурацияланған құқықтар жиынтығымен бірге пайдалана аласыз немесе рөлдер жасай аласыз және қажетті құқықтарды өзіңіз конфигурациялай аласыз.

Бағдарлама функцияларына қатынасу құқықтары

Төмендегі кестеде тапсырмаларды, есептерді, параметрлерді басқаруға және пайдаланушы әрекеттерін орындауға құқық беретін Kaspersky Security Center функциялары берілген.

Кестеде көрсетілген пайдаланушы әрекеттерін орындау үшін пайдаланушының әрекеттің жанында көрсетілген құқығы болуы керек.

Оқу, **Жазу** және **Орындау** құқықтары кез келген тапсырмаға, есепке немесе параметрге қолданылады. Осы құқықтармен қоса, құрылғы таңдауларында тапсырмаларды, есептерді немесе параметрлерді басқару үшін пайдаланушыда **Құрылғылардың таңдауларында әрекеттерді орындау** құқығы болуы керек.

> Кестеде жоқ барлық тапсырма, есеп, параметр және орнату пакеті **Жалпы функционал: Базалық функционалдылық** функционалдық аймағына жатады.

Бағдарлама функцияларына қатынасу құқықтары

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
Жалпы функционал: **Басқару топтарын басқару**	**Жазу**	• Құрылғыны басқару тобына қосу: **Жазу** • Басқару тобынан құрылғыны жою: **Жазу** • Басқа басқару тобына басқару қосутобын қосыңыз: **Жазу** • Басқа басқару тобынан басқару тобын жою: **Жазу**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
Жалпы функционал: ACL тізіміне қарамастан, нысандарға қатынасу	**Оқу**	Барлық нысанға Оқу рұқсат алу: **Оқу**	Жоқ	Жоқ	**Жалпы функционал: AC тізіміне қарамастан, нысандарға қатынасу** аудит мақсаттарына арналған. Пайдаланушылар осы функционал аймақта **Оқу** құқықтары берілгенде, олар барлық нысанға толық **Оқу** рұқса алады және жергілікті әкімші құқықтары бар (L жүйесіне арналғ түбір) желілік аге арқылы басқару серверіне қосыл құрылғыларды таңдау бойынша келген жасалған тапсырманы орындай алады. құқықтарды қызметтік міндеттерін оры үшін қажет пайдаланушылар шектеулі жинағы мұқият беру ұсынылады. Кіру рұқсаты бас құқықтарға қарамастан бері (тіпті олар белгіл нысандарды Оқу тыйым салса да)
Жалпы функционал: **Базалық функционалдылық**	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Виртуалды серверге арналған құрылғыны жылжыту ережелері (жасау, өзгерту немесе жою): **Жазу**, **Құрылғылардың таңдауларында әрекеттерді орындау** • Мобильдік (LWNGT) протоколдың арнаулы сертификатын алу: **Оқу** • Мобильдік (LWNGT) протоколдың арнаулы сертификатын орнату: **Жазу** • NLA анықталған желі тізімін алу: **Оқу** • NLA анықталған желі тізімін қосу, өзгерту немесе жою: **Жазу** • Көру рұқсатын басқару топтарының тізімі: **Оқу**	• "Жаңартуларды Басқару серверінің қоймасына жүктеп алу" • "Есептерді жеткізу" • "Орнату пакеттерін тарату" • "Қосалқы Басқару серверлеріне бағдарламаларды орнату"	• "Қорғаныс жағдайы туралы есеп" • "Қауіп-қатер туралы есеп" • "Ең көп зақымдалған құрылғылар туралы есеп" • "Антивирустық дерекқордың күйі туралы есеп" • "Қателер туралы есеп" • "Желілік шабуылдар туралы есеп" • "Пошталық жүйелерді қорғауға арналған бағдарламалар туралы жиынтық есеп" • "Периметрді қорғайтын бағдарламалар туралы жиынтық есеп"	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
		• Kaspersky оқиғалар журналын көру: **Оқу** • BitLocker арқылы шифрланған қатқыл дискіге кіруді қалпына келтіру үшін қалпына келтіру кілтін көру: **Орындау**		• "Орнатылған бағдарлама түрлері туралы жиынтық есеп" • "Вирус жұққан құрылғылардың пайдаланушылары туралы есеп" • "Инциденттер туралы есеп" • "Оқиғалар туралы есеп" • "Тарату нүктелерінің әрекетіндегі есеп" • "Қосалқы Басқару серверлері туралы есеп" • "Құрылғыларды басқару оқиғалары туралы есеп" • "Осалдықтар туралы есеп" • "Рұқсат берілмеген бағдарламалар бойынша есеп" • "Веб-бақылау туралы есеп" • "Басқарылатын құрылғыларды шифрлаудың күйі туралы есеп" • "Жаппай сақтау құрылғыларын шифрлау күйі туралы есепті көру" • "Файлдарды шифрлау қателері туралы есеп" • "Шифрланған файлдарға қатынасты бұғаттау туралы есеп" • "Шифрланған құрылғыларға қатынасу құқықтары туралы есеп" • "Пайдаланушының тиімді құқықтары туралы есеп" • "Құқықтар туралы есеп"	
Жалпы функционал: **Жойылған нысандар**	• **Оқу** • **Жазу**	• Себеттегі жойылған нысандарды көру: **Оқу** • Себеттен нысандарды жою: **Жазу**	Жоқ	Жоқ	Жоқ
Жалпы функционал: **Оқиғаларды өңдеу**	• **Оқиғалар жойылуда** • **Оқиғаның хабарландыру параметрлерін өңдеу**	• Оқиғаларды тіркеу параметрлерін өзгерту: **Оқиғаларды тіркеу параметрлерін өңдеу** • Оқиғалар туралы хабарландыру параметрлерін	Жоқ	Жоқ	Параметрлер: • Вирустық шабуыл параметрле вирустық шабуыл оқиғасын жа үшін қажетті

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
	• **Оқиғаларды тіркеу параметрлерін өңдеу** • **Жазу**	өзгерту: **Оқиғаның хабарландыру параметрлерін өңдеу** • Оқиғаларды жою: **Оқиғалар жойылуда**			вирусты анықтау сан • Вирустық шабуыл параметрле вирусты анықтауды бағалау кезе • Дерекқорда сақталатын оқиғалардың максималды саны • Қашықтағы құрылғылард оқиғаларын сақтау кезең
Жалпы функционал: **Басқару серверіне қатысты әрекеттер**	• **Оқу** • **Жазу** • **Орындау** • **Нысан ACL параметрлерін өзгерту** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Желілік агент қосылымы үшін басқару серверінің порттарын көрсету: **Жазу** • Басқару серверінде іске қосылған белсендіру прокси порттарын көрсету: **Жазу** • Басқару серверінде іске қосылған мобильдік телефонға арналған белсендіру прокси порттарын көрсету: **Жазу** • Оқшау пакеттерді тарату үшін веб-сервер порттарын көрсету: **Жазу** • MDM профильдерін тарату үшін веб-сервер порттарын көрсету: **Жазу** • Kaspersky Security Center Web Console арқылы қосылу үшін басқару серверінің SSL порттарын көрсету: **Жазу** • Мобильдік байланыс үшін басқару серверінің порттарын көрсету: **Жазу** • Басқару сервері дерекқорында сақталған оқиғалардың максималды санын көрсету: **Жазу** • Басқару сервері жібере алатын оқиғалардың максималды санын көрсету: **Жазу** • Басқару сервері оқиғаларды жібере алатын уақыт аралығын көрсету: **Жазу**	• "Басқару сервері деректерінің сақтық көшірмесін жасау" • "Дерекқорларға қызмет көрсету"	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
Жалпы функционал: **Kaspersky қолданбасын енгізу**	• **Kaspersky патчтарын басқару** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	Патч орнатуды мақұлдау немесе қабылдамау: **Kaspersky патчтарын басқару**	Жоқ	• "Виртуалды Басқару серверінің лицензиялық кілтін пайдалануы туралы есеп" • "Kaspersky бағдарламалық жасақтамасының нұсқалары туралы есеп" • "Үйлесімсіз қосымшалар туралы есеп" • "Kaspersky бағдарламалық жасақтама модулі жаңартуларының нұсқалары туралы есеп" • "Қорғаныс орналастыру туралы есеп"	Орнату пакеті: Kaspersky.
Жалпы функционал: **Лицензиялық кілттерді басқару**	• **Кілт файлын экспорттау** • **Жазу**	• Кілт файлын экспорттау: **Кілт файлын экспорттау** • Басқару серверінің лицензия кілтінің параметрлерін өзгерту: **Жазу**	Жоқ	Жоқ	Жоқ
Жалпы функционал: **Есеп файлын мәжбүрлеп басқару**	• **Оқу** • **Жазу**	• ACL-ге қарамастан есептерді жасау: **Жазу** • ACL-ге қарамастан есептерді орындау: **Оқу**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
Жалпы функционал: **Басқару серверлерінің иерархиясы**	**Басқару серверлерінің иерархиясын конфигурациялау**	Қосалқы басқару серверлерін тіркеу, жаңарту немесе жою: **Басқару серверлерінің иерархиясын конфигурациялау**	Жоқ	Жоқ	Жоқ
Жалпы функционал: **Пайдаланушы рұқсаттары**	**Нысан ACL параметрлерін өзгерту**	• Кез келген нысанның қауіпсіздігі сипаттарын өзгерту: **Нысан ACL параметрлерін өзгерту** • Пайдаланушы рөлдерін басқару: **Нысан ACL параметрлерін өзгерту** • Ішкі пайдаланушыларды басқару: **Нысан ACL параметрлерін өзгерту** • Қауіпсіздік топтарын басқару: **Нысан ACL параметрлерін өзгерту** • Бүркеншік аттарды басқару: **Нысан ACL параметрлерін өзгерту**	Жоқ	Жоқ	Жоқ
Жалпы функционал: **Виртуалды Басқару серверлері**	• **Виртуалды Басқару серверлерін басқару** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Виртуалды басқару серверлерінің тізімін алу: **Оқу** • Виртуалды басқару сервері туралы ақпаратты алу: **Оқу** • Виртуалды басқару серверін жасау, жаңарту немесе жою: **Виртуалды Басқару серверлерін басқару** • Виртуалды басқару серверін басқа топқа жылжыту: **Виртуалды Басқару серверлерін басқару** • Виртуалды басқару сервері рұқсаттарын орнату: **Виртуалды Басқару серверлерін басқару**	Жоқ	Үшінші тарап бағдарламалық жасақтамасы жаңартуларын орнату нәтижелерін хабарлау.	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
Жалпы функционал: **Шифрлау кілтін басқару**	**Жазу**	Шифрлау кілттерін импорттау: **Жазу**	Жоқ	Жоқ	Жоқ
Мобильді құрылғыларды басқару: Жалпы	• **Жаңа құрылғыларды қосу** • **Ұялы құрылғыларға тек ақпараттық пәрмендерді жіберу** • **Ұялы құрылғыларға пәрмендер жіберу** • **Сертификаттарды басқару** • **Оқу** • **Жазу**	• Key Management Service қалпына келтіру деректерін алу: **Оқу** • Пайдаланушы сертификаттарын жою: **Сертификаттарды басқару** • Пайдаланушы сертификатының жалпы бөлігін алу: **Оқу** • Ашық кілт инфрақұрылымы қосылғанын тексеру: **Оқу** • Ашық кілт инфрақұрылымы есептік жазбасын тексеру: **Оқу** • Ашық кілт инфрақұрылымының үлгілерін алу: **Оқу** • Кеңейтілген кілтті пайдалану сертификаты арқылы ашық кілт инфрақұрылымының үлгілерін алу: **Оқу** • Ашық кілт инфрақұрылымы сертификатының күші жойылғанын тексеру: **Оқу** • Пайдаланушы сертификатын шығару параметрлерін жаңарту: **Сертификаттарды басқару** • Пайдаланушы сертификатын шығару параметрлерін алу: **Оқу** • Қолданба атауы мен нұсқасы бойынша пакеттерді алу: **Оқу** • Пайдаланушы сертификатын орнату немесе одан бас тарту: **Сертификаттарды басқару** • Пайдаланушы сертификатын жаңарту: **Сертификаттарды басқару**	Жоқ	Жоқ	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
		• Пайдаланушы сертификатының тэгін орнату: **Сертификаттарды басқару** • MDM орнату пакетін қайта жасауды іске қосу; MDM орнату пакетін жасаудан бас тарту: **Жаңа құрылғыларды қосу**			
Жүйені басқару: Қосылым мүмкіндігі	• **RDP сеанстарын бастау** • **Бұрыннан бар RDP сеанстарына қосылу** • **Туннельдеуді бастау** • **Құрылғылардағы файлдарды әкімшінің жұмыс станциясында сақтау** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Жұмыс үстелін бөлісу сеансын жасау: **RDP сеанстарын бастау** • RDP сеансын жасау: **Бұрыннан бар RDP сеанстарына қосылу** • Туннель жасау: **Туннельдеуді бастау** • Мазмұн желісінің тізімін сақтау: **Құрылғылардағы файлдарды әкімшінің жұмыс станциясында сақтау**	Жоқ	"Құрылғы пайдаланушылары туралы есеп"	Жоқ
Жүйені басқару: Жабдықты түгендеу	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Аппараттық жасақтаманы түгендеу нысанын алу немесе экспорттау: **Оқу** • Аппараттық жасақтаманы түгендеу нысандарын қосу, орнату немесе жою: **Жазу**	Жоқ	• "Жабдық тізімдемесі туралы есеп" • "Конфигурацияны өзгерту туралы есеп" • "Жабдық туралы есеп"	Жоқ
Жүйені басқару: Желіге қатынасты басқару	• **Оқу** • **Жазу**	• CISCO параметрлерін көру: **Оқу** • CISCO параметрлерін өзгерту: **Жазу**	Жоқ	Жоқ	Жоқ
Жүйені басқару: Операциялық жүйені орналастыру	• **PXE серверлерін жаю** • **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• PXE серверлерін орналастыру: **PXE серверлерін жаю** • PXE серверлерінің тізімін көру: **Оқу** • PXE клиенттерінде орнату процесін бастау немесе тоқтату: **Орындау** • WinPE және операциялық жүйе кескіндері үшін драйверлерді басқару: **Жазу**	"Анықтамалық құрылғының ОЖ кескінінің орнату пакетін жасау"	Жоқ	Орнату пакеттер "Операциялық ж кескіні"
Жүйені басқару: Осалдықтар мен патчтарды басқару	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Үшінші тарап патч сипаттарын көру: **Оқу** • Үшінші тарап патч сипаттарын өзгерту: **Жазу**	• "Windows Update жаңартуларын синхрондауды орындау" • "Windows Update жаңартуларын орнату"	"Бағдарламалық жасақтаманың жаңартулары туралы есеп"	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
			• "Осалдықтарды түзету" • "Қажетті жаңартуларды орнату және осалдықтарды түзету"		
Жүйені басқару: Қашықтан орнату	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	• Үшінші тараптың осалдықтар мен патчтарды басқару негізіндегі орнату пакетінің сипаттарын көру: **Оқу** • Үшінші тараптың салдықтар мен патчтарды басқару негізіндегі орнату пакетінің сипаттарын өзгертіңіз: **Жазу**	Жоқ	Жоқ	Орнату пакеттер • "Пайдаланушы бағдарламас • "Орнату пак
Жүйені басқару: Бағдарламалық жасақтамаларды түгендеу	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	Жоқ	Жоқ	• "Орнатылған бағдарламалар туралы есеп" • "Өтінімдер тізілімі туралы есеп журналы" • "Лицензияланған бағдарламалар топтарының күйі туралы есеп" • "Үшінші тарап бағдарламалық жасақтамасының лицензиялық кілттері туралы есеп"	Жоқ

Функционалдық аймақ	Құқық	Пайдаланушының әрекеті: әрекетті орындауға қажетті құқық	Тапсырма	Есеп	Басқа
Жүйені басқару: Сценарийлерді қашықтан іске қосу	• **Оқу** • **Жазу** • **Орындау** • **Құрылғылардың таңдауларында әрекеттерді орындау**	Пайдаланушы тапсырма сипаттарын көре алады: **Оқу** Пайдаланушы орнату пакетін жасай, жоя немесе өзгерте алады: **Жазу** Пайдаланушы тапсырманы орындай алады: **Жазу**. Linux операциялық жүйесімен жұмыс істейтін клиенттік құрылғыларда скриптілер root құқықтарымен орындалады. Пайдаланушы тапсырманы іске қоса алады немесе оны орындауды жоспарлай алады: **Орындау** Пайдаланушы құрылғылар жинағында тапсырманы іске қоса алады: **Құрылғылардың таңдауларында әрекеттерді орындау**	"Скрипттерді қашықтан орындау"	Жоқ	Жоқ

Алдын ала анықталған пайдаланушы рөлдері

Kaspersky Security Center пайдаланушыларына тағайындалған пайдаланушы рөлдері оларға бағдарламаның функцияларына қатынасу құқықтарының жиынтығын береді.

Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Конфигурацияланған құқықтар жинағы бар алдын ала анықталған пайдаланушы рөлдерін пайдалануға немесе жаңа рөлдер жасауға болады. Жаңа рөл жасаған кезде, рөл ауқымын өзіңіз орнатуыңыз және пайдалану құқықтарын Kaspersky Security Center мүмкіндіктеріне тағайындауыңыз керек. Kaspersky Security Center-де қолжетімді пайдаланушылардың кейбір алдын ала анықталған рөлдері **Аудитор**, **Қауіпсіздік қызметінің офицері**, **Супервайзер** сияқты белгілі бір лауазымдармен байланысты болуы мүмкін (бұл рөлдер Kaspersky Security Center бағдарламасында 11-нұсқадан бастап бар). Бұл рөлдерге қатынасу құқықтары тиісті лауазымдардың стандартты тапсырмалары мен міндеттеріне сәйкес алдын ала конфигурацияланады. Төмендегі кестеде рөлдердің белгілі бір лауазымдармен қалай байланысты болуы мүмкін екендігі көрсетілген.

Белгілі бір лауазымдарға арналған рөлдердің мысалдары

Рөл	Пікір
Аудитор	Басқару серверіне жергілікті әкімші құқықтары (Linux жүйесіне арналған түбір) бар желілік агент арқылы қосылған құрылғылар жинағында барлық көру операциясына және жасалған тапсырмаларды орындауға рұқсат береді. Бұл қызметтік міндеттерді орындау үшін осы рөлді пайдаланушылардың шектеулі жинағына мұқият тағайындауға кеңес береміз.
Супервайзер	Барлық операцияларды қарауға рұқсат етіледі, басқа операцияларға рұқсат етілмейді. Сіз бұл рөлді қауіпсіздік қызметінің офицеріне және ұйымыңыздағы IT қауіпсіздігіне жауап беретін басқа менеджерлерге тағайындай аласыз.
Қауіпсіздік қызметінің офицері	Барлық қарау операцияларына рұқсат етіледі, есептерді басқаруға рұқсат етіледі; **Жүйені басқару**: **Қосылым мүмкіндігі** аймағындағы шектулі құқықтар ұсынған. Сіз бұл рөлді ұйымыңыздағы IT қауіпсіздігіне жауапты қызметкерге тағайындай аласыз.

Төмендегі кестеде пайдаланушының әрбір алдын ала анықталған рөліне арналған құқықтар келтірілген.

Пайдаланушылардың алдын ала анықталған рөлдерінің құқықтары

Рөл	Сипаттамасы
Басқару серверінің әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Оқиғаларды өңдеу** • **Басқару серверлерінің иерархиясы** • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Қосылымдар** • **Жабдықты түгендеу** • **Бағдарламалық жасақтамаларды түгендеу** **Жалпы мүмкіндіктер: Шифрлау кілтін басқару** функционалды аймағында **Оқу** және **Жазу** құқықтарын береді.
Басқару серверінің операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Қосылымдар** • **Жабдықты түгендеу** • **Бағдарламалық жасақтамаларды түгендеу**
Аудитор	**Жалпы функционал** функционалдық аймағында барлық операцияларға рұқсат береді: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Жойылған нысандар** • **Есептерді басқару** Сіз бұл рөлді ұйымыңыздың аудитін жүргізетін қызметкерге тағайындай аласыз.

Рөл	Сипаттамасы
Бағдарламаларды орнату әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Kaspersky бағдарламалық жасақтамасын орналастыру** • **Лицензиялық кілттерді басқару** • **Жүйені басқару**: • **Операциялық жүйені орналастыру** • **Осалдықтар мен патчтарды басқару** • **Қашықтан орнату** • **Бағдарламалық жасақтамаларды түгендеу** **Жалпы функционал: Базалық функционалдылық** аймағында **Оқу** және **Орындау** құқықтарын ұсынады.
Бағдарламаларды орнату операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Kaspersky бағдарламалық жасақтамасын орналастыру** (сондай-ақ осы аймақта **Kaspersky патчтарын басқару** құқығын береді) • **Виртуалды Басқару серверлері** • **Жүйені басқару**: • **Операциялық жүйені орналастыру** • **Осалдықтар мен патчтарды басқару** • **Қашықтан орнату** • **Бағдарламалық жасақтамаларды түгендеу**
Kaspersky Endpoint Security әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы **Жалпы мүмкіндіктер: Шифрлау кілтін басқару** функционалды аймағында **Оқу** және **Жазу** құқықтарын береді.
Kaspersky Endpoint Security операторы	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** құқықтарын ұсынады: • **Жалпы функционал: Базалық функционал** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы
Бас әкімші	Келесі аймақтарды *қоспағанда*, функционалдық аймақтардағы барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Есептерді басқару** **Жалпы мүмкіндіктер: Шифрлау кілтін басқару** функционалды аймағында **Оқу** және **Жазу** құқықтарын береді.

Рөл	Сипаттамасы
Бас оператор	Барлық келесі функционалдық аймақтарда **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады: • **Жалпы функциялар**: • **Базалық функционалдылық** • **Жойылған нысандар** • **Басқару серверіне қатысты әрекеттер** • **Kaspersky қолданбасын енгізу** • **Виртуалды Басқару серверлері** • **Ұялы құрылғыларды басқару: Жалпы** • Барлық функцияларды қосқанда, **Жүйені басқару** • Барлық функцияларды қоса алғанда, Kaspersky Endpoint Security аймағы
Ұялы құрылғыларды басқару әкімшісі	Келесі функционалдық аймақтардағы барлық операцияларға рұқсат береді: • **Жалпы функционал: Базалық функционал** • **Ұялы құрылғыларды басқару: Жалпы**
Ұялы құрылғыларды басқару операторы	**Жалпы функционал**: **Базалық функционалдылық** аймағында **Оқу** және **Орындау** құқықтарын ұсынады. Келесі функционалдық аймақта **Оқу** және **Ұялы құрылғыларға тек ақпараттық пәрмендерді жіберу** құқықтарын ұсынады: **Ұялы құрылғыларды басқару**: **Жалпы**.
Қауіпсіздік қызметінің офицері	Келесі функционалдық аймақтарда барлық операцияларға рұқсат береді: **Жалпы функционал**: • **ACL тізіміне қарамастан, нысандарға қатынасу** • **Есептерді басқару** **Жүйені басқару: Қосылымдар** аймағында **Оқу**, **Жазу**, **Орындау**, **Құрылғылардағы файлдарды әкімшінің жұмыс орнында сақтау** және **Құрылғылардың таңдауларында әрекеттерді орындау** құқықтарын ұсынады. Сіз бұл рөлді ұйымыңыздағы IT қауіпсіздігіне жауапты қызметкерге тағайындай аласыз.
Self Service Portal пайдаланушысы	**Ұялы құрылғыларды басқару: Self Service Portal** аймағында барлық операцияларға рұқсат береді. Бұл функцияға Kaspersky Security Center 11 және одан жоғары нұсқаларында қолдау көрсетілмейді.
Супервайзер	**Жалпы функционал**: **ACL тізіміне қарамастан, нысандарға қатынасу** және **Жалпы функционал**: **Есептерді басқару** функционалдық аймағының аймағында **Оқу** құқықтарын ұсынады. Сіз бұл рөлді қауіпсіздік қызметінің офицеріне және ұйымыңыздағы IT қауіпсіздігіне жауап беретін басқа менеджерлерге тағайындай аласыз.
Осалдықтар мен патчтарды басқару әкімшісі	**Жалпы функционал**: **Базалық функционалдылық** және **Жүйені басқару** (барлық функцияларды қоса алғанда) аймағындағы барлық операцияларға рұқсат береді.
Осалдықтар мен патчтарды басқару операторы	**Жалпы функционал**: **Базалық функционалдылық** және **Жүйені басқару** (барлық функцияларды қоса алғанда) аймағында **Оқу** және **Орындау** (қолданылса) құқықтарын ұсынады.

Нысандар жиынтығына қатынасу құқықтарын тағайындау

Сервер деңгейінде қатынасу құқықтарын тағайындауға қосымша ретінде, сіз нақты нысандарға, мысалы, қажетті тапсырмаға қатынасу мүмкіндігін тағайындай аласыз. Бағдарлама келесі нысан түрлеріне қатынасу құқықтарын көрсетуге мүмкіндік береді:

- Басқару топтары
- Тапсырмалар
- Есептер

- Құрылғыны таңдаулары
- Оқиғалар таңдау

Нақты нысанға қатынасу құқықтарын тағайындау үшін:

1. Нысанның түріне байланысты, басты мәзірде тиісті бөлімге өтіңіз:
   - **Активтер (құрылғылар)** → **Топтардың иерархиясы**.
   - **Активтер (құрылғылар)** → **Тапсырмалар**.
   - **Бақылау және есеп беру** → **Есептер**.
   - **Активтер (құрылғылар)** → **Құрылғы таңдаулары**.
   - **Бақылау және есеп беру** → **Оқиғаларды таңдау**.
2. Қатынасу құқықтарын тағайындағыңыз келетін нысанның сипаттарын ашыңыз.

   Басқару тобының немесе тапсырманың сипаттары терезесін ашу үшін, нысанның атауын басыңыз. Басқа нысандардың сипаттарын құралдар тақтасындағы түйменің көмегімен ашуға болады.
3. Сипаттар терезесінде **Қатынасу құқықтары** бөлімін ашыңыз.

   Пайдаланушылар тізімі ашылады. Атап көрсетілген пайдаланушылар мен қауіпсіздік топтарының нысанға қатынасу құқықтары бар. Басқару топтарының немесе Серверлердің иерархиясын қолданып жатсаыз, әдепкі бойынша тізім мен қатынасу құқықтары тектік басқару тобынан немесе басты Серверден иеленеді.
4. Тізімді өзгерту мүмкіндігіне ие болу үшін **Реттелетін рұқсаттарды пайдалану** параметрін қосыңыз.
5. Қатынасу құқықтарын конфигурациялаңыз:
   - Тізімді өзгерту үшін **Қосу** және **Жою** түймелерін қолданыңыз.
   - Пайдаланушы немесе басқару топтары үшін қатынасу құқықтарын көрсетіңіз. Келесі әрекеттердің бірін орындаңыз:
     - Егер сіз қатынасу құқықтарын қолмен көрсеткіңіз келсе, пайдаланушыны немесе қауіпсіздік тобын таңдап, **Қатынасу құқықтары** түймесін басып, қатынасу құқықтарын көрсетіңіз.
     - Пайдаланушыға немесе қауіпсіздік тобына пайдаланушы рөлін тағайындағыңыз келсе, пайдаланушыны немесе қауіпсіздік тобын таңдап, **Рөлдер** түймесін басыңыз және тағайындалатын рөлді таңдаңыз.
6. **Сақтау** түймесін басыңыз.

Нысанға қатынасу құқықтары конфигурацияланған.

Пайдаланушыларға немесе қауіпсіздік топтарына құқықтарды тағайындау

Басқару серверінің әртүрлі мүмкіндіктерін пайдалану үшін пайдаланушыларға немесе қауіпсіздік топтарына кіру құқықтарын тағайындауға болады, мысалы, Kaspersky Endpoint Security for Linux.

Пайдаланушыға немесе қауіпсіздік тобына құқықтарды тағайындау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Қатынасу құқықтары** қойындысында құқық тағайындағыңыз келетін пайдаланушы немесе қауіпсіздік тобы атының жанындағы жалаушаны белгілеп, **Қатынасу құқықтары** түймесін басыңыз.

   Бір уақытта бірнеше пайдаланушыны немесе қауіпсіздік тобын таңдау мүмкін емес. Бірнеше нысанды таңдасаңыз, **Қатынасу құқықтары** түймесі өшірулі болады.

3. Пайдаланушы немесе топ үшін құқықтар жинағын орнатыңыз:

   a. Түйінді Басқару сервер немесе басқа Kaspersky бағдарламасының функцияларымен кеңейтіңіз.

   b. Қажетті функцияның немесе қол жеткізу құқығының жанындағы **Рұқсат** немесе **Тыйым салу** жалаушасын белгілеңіз.

      1-мысал: пайдаланушыға немесе топқа бағдарламаны біріктіру функциясына (**Оқу**, **Жазу** және **Орындау**) барлық қолжетімді қол жеткізу құқықтарын беру үшін **Бағдарлама интеграциялары** түйінінің жанындағы **Рұқсат ету** жалаушасын белгілеңіз.

      2-мысал: **Шифрлау кілттерін басқару** түйінін кеңейтіңіз және пайдаланушыға немесе топқа шифрлау кілттерін басқару функциясына **жазу** құқығын беру үшін **Жазу** рұқсатының жанындағы **Рұқсат ету** жалаушасын белгілеңіз.

4. Қол жеткізу құқықтарының жинағын орнатқаннан кейін **OK** түймесін басыңыз.

Пайдаланушы немесе пайдаланушылар тобы үшін құқықтар жиынтығы конфигурацияланған.

Басқару серверінің (немесе басқару тобының) құқықтары келесі аймақтарға бөлінеді:

- Жалпы функционал:
  - Басқару топтарын басқару
  - ACL тізіміне қарамастан, нысандарға қатынасу
  - Базалық функционалдылық
  - Жойылған нысандар
  - Шифрлау кілтін басқару
  - Оқиғаларды өңдеу
  - Басқару серверіне қатысты әрекеттер (тек Басқару сервері сипаттары терезесінде)
  - Құрылғы тегтері
  - Kaspersky қолданбасын енгізу
  - Лицензиялық кілттерді басқару
  - Бағдарламаны біріктіру
  - Есеп файлын мәжбүрлеп басқару

    - Басқару серверлерінің иерархиясы
    - Пайдаланушы рұқсаттары
    - Виртуалды Басқару серверлері
- Мобильді құрылғыларды басқару:
    - Жалпы
    - Self Service Portal
- Жүйені басқару:
    - Қосылым мүмкіндігі
    - Сценарийлерді қашықтан іске қосу
    - Жабдықты түгендеу
    - Желіге қатынасты басқару
    - Операциялық жүйені орналастыру
    - Осалдықтар мен патчтарды басқару
    - Қашықтан орнату
    - Бағдарламалық жасақтамаларды түгендеу

Құқық үшін не **Рұқсат**, не **Тыйым салу** таңдалмаса, ол *анықталмаған* болып саналады: құқық пайдаланушы үшін айқын түрде қабылданбайынша немесе рұқсат етілмейінше қабылданбайды.

Пайдаланушылардың құқықтары келесінің жиынтығы болып саналады:

- Пайдаланушының өзіндік құқықтары
- Пайдаланушыға тағайындалған барлық рөлдердің құқықтары
- Пайдаланушы кіретін барлық қауіпсіздік топтарының құқықтары
- Пайдаланушы кіретін топтарға тағайындалған барлық рөлдердің құқықтары

Ең болмаса бір құқықтар жиынтығында тыйым салынған құқық болса (құқық үшін **Тыйым салу** жалаушасы қойылған), онда бұл құқық басқа құқықтар жиынтығында рұқсат етілген немесе анықталмаған болса да, пайдаланушы үшін тыйым салынған болып саналады.

Сондай-ақ, Басқару серверінің әртүрлі мүмкіндіктерін пайдалану үшін пайдаланушы рөлі аймағына пайдаланушылар мен қауіпсіздік топтарын қосуға болады. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Ішкі пайдаланушының есептік жазбасын қосу

Пайдаланушының есептік жазбасын қосқыңыз келсе, есептік жазбаңызда "Жалпы функционал: Пайдаланушылардың құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар екенін тексеріңіз.

Kaspersky Security Center жаңа пайдаланушы есептік жазбасын қосу үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

2. **Қосу** түймесін басыңыз.

3. Ашылған **Пайдаланушыны қосу** терезесінде жаңа пайдаланушы параметрлерін көрсетіңіз:

   - **Атауы**

   - **Құпиясөз**

     Құпиясөз келесі ережелерге сәйкес келуі керек:

     - Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.

     - Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:

       - Бас әріптер (A-Z)

       - Кіші әріптер (a-z)

       - Сандар (0-9)

       - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

     - Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

     Енгізілген құпиясөзді көру үшін түймесін басыңыз.

     Пайдаланушының бірінші аутентификациясында құпиясөзді өзгертуге мәжбүрлеу үшін **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрін қосуға болады.

4. Пайдаланушы есептік жазбасын жасауды аяқтау үшін өзгерістерді сақтаңыз.

Пайдаланушының есептік жазбасы пайдаланушылар тізіміне қосылды.

Kaspersky Security Center Web Console веб-консолінде жасалған ішкі пайдаланушы есептік жазбасымен кіру үшін есептік жазбаға рөл тағайындауыңыз керек. Кірмес бұрын, ішкі пайдаланушы есептік жазбасында рөл бар екеніне көз жеткізіңіз. Әйтпесе, кіру қатесі орын алады.

Пайдаланушылар тобын жасау

Қауіпсіздік тобын жасау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Топтар** қойындысын таңдаңыз.
2. **Қосу** түймесін басыңыз.
3. Ашылатын **Қауіпсіздік тобын жасау** терезесінде жаңа қауіпсіздік тобы үшін келесі параметрлерді көрсетіңіз:
   - **Топ атауы**
   - **Сипаттама**
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Қауіпсіздік тобы топтар тізіміне қосылды.

Ішкі пайдаланушының есептік жазбасын өзгерту

Пайдаланушының есептік жазбасын өзгерткіңіз келсе, есептік жазбаңызда "Жалпы функционал: Пайдаланушылардың құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар екенін тексеріңіз.

Kaspersky Security Center ішкі пайдаланушы есептік жазбасын өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Өзгерту қажет болған реттелетін есептік жазбасын таңдаңыз.
3. Ашылған терезедегі **Жалпы** қойыншасында пайдаланушы есептік жазбасының параметрлерін өзгертіңіз:
   - **Пайдаланушы күйі**

     Қажет болса, пайдаланушының бағдарламаға қосылуына тыйым салу үшін қосқышты **Өшірулі** күйіне ауыстырыңыз. Мысалы, қызметкер компаниядан жұмыстан шыққаннан кейін, есептік жазбаны өшіруге болады.
   - **Атауы**
   - **Толық атауы**
   - **Сипаттама**
   - **Электрондық пошта мекенжайы**
   - **Негізгі телефон нөмірі**

- **Құпиясөз**

  Қажет болса, пайдаланушыны Kaspersky Security Center орталығына қосу үшін келесі әдіспен жаңа құпиясөз орнатуға болады:

  a. **Құпиясөзді өзгерту** түймесін басып, пайдаланушы есептік жазбасы үшін жаңа құпиясөз орнатыңыз.

  Құпиясөз келесі ережелерге сәйкес келуі керек:

  - Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
  - Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
    - Бас әріптер (A-Z)
    - Кіші әріптер (a-z)
    - Сандар (0-9)
    - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

  Енгізілген құпиясөзді көру үшін түймесін басыңыз.

  b. Қажет болса, пайдаланушының келесі аутентификациясында құпиясөзді өзгертуге мәжбүрлеу үшін **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрін қосыңыз.

  c. Егер пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде "Жалпы функционал: Пайдаланушылар құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар есептік жазба деректерін көрсетіңіз.

4. **Аутентификация қауіпсіздігі** қойыншасында осы есептік жазбаға арналған қауіпсіздік параметрлерін көрсете аласыз.

5. **Топтар** қойыншасында пайдаланушыны немесе қауіпсіздік тобын қосуға болады.

6. **Құрылғылар** қойыншасында пайдаланушыға құрылғыларды тағайындауға болады.

7. **Рөлдер** қойыншасында пайдаланушыға рөлді тағайындауға болады.

8. Пайдаланушы есептік жазбасын өзгертуді аяқтау үшін өзгерістерді сақтаңыз.

Өзгертілген пайдаланушы есептік жазбасы пайдаланушылар тізімінде көрсетіледі.

Пайдаланушылар тобын өзгерту

Қауіпсіздік тобын өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Топтар** қойындысын таңдаңыз.

2. Өзгерту қажет қауіпсіздік тобын таңдаңыз.

3. Ашылған терезеде қауіпсіздік тобының параметрлерін өзгертіңіз:

   - **Жалпы** қойындысында **Атауы** және **Сипаттама** параметрлерін өзгертуге болады. Бұл параметрлер тек ішкі қауіпсіздік топтары үшін қолжетімді.
   - **Пайдаланушылар** қойындысында пайдаланушыларды қауіпсіздік тобына қосуға болады. Бұл параметрлер тек ішкі пайдаланушыларға және ішкі қауіпсіздік топтарына қолжетімді.
   - **Рөлдер** қойындысында қауіпсіздік тобына рөл тағайындай аласыз.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Өзгерістер қауіпсіздік тобына қолданылды.

Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау

Пайдаланушыға немесе қауіпсіздік тобына рөл тағайындау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** немесе **Топтар** қойындысын таңдаңыз.
2. Рөл тағайындағыңыз келетін пайдаланушының немесе қауіпсіздік тобының атын таңдаңыз.

   Бірнеше ат таңдауға болады.
3. Мәзірде **Рөлді тағайындау** түймесін басыңыз.

   Рөлді тағайындау шебері іске қосылады.
4. Шебер нұсқауларын орындаңыз: таңдалған пайдаланушыларға немесе қауіпсіздік топтарына тағайындағыңыз келетін рөлді таңдаңыз және рөлдің әрекет ету ауқымын таңдаңыз.

   Пайдаланушы рөлі ауқымы – бұл пайдаланушылар мен басқару топтарының тіркесімі. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Нәтижесінде Басқару сервермен жұмыс істеу құқықтарының жиынтығы бар рөл пайдаланушыға (немесе пайдаланушылар тобына не қауіпсіздік тобына) тағайындалады. Пайдаланушылар немесе қауіпсіздік топтарының тізімінде **Тағайындалған рөлдері бар** бағанында жалауша көрсетіледі.

Виртуалды серверде жасалған пайдаланушыларға басқару серверінде рөлдерді тағайындау мүмкін емес.

Пайдаланушылардың есептік жазбаларын ішкі қауіпсіздік топқа қосу

Ішкі пайдаланушылар есептік жазбаларын тек ішкі қауіпсіздік тобына қосуға болады.

Пайдаланушылардың есептік жазбаларын қауіпсіздік тобына қосу үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Қауіпсіздік тобына қосқыңыз келетін пайдаланушылардың есептік жазбаларына қарама-қарсы жалаушаларды белгілеңіз.

3. **Топты тағайындау** түймесін басыңыз.

4. **Топты тағайындау** ашылған терезесінде пайдаланушылардың есептік жазбаларын қосу қажет қауіпсіздік тобын таңдаңыз.

5. **Сақтау** түймесін басыңыз.

Пайдаланушылардың есептік жазбалары қауіпсіздік тобына қосылған. Ішкі пайдаланушыларды қауіпсіздік тобына топ параметрлері арқылы да қосуға болады.

Пайдаланушыны құрылғының иесі етіп тағайындау

Пайдаланушыны мобильдік құрылғының иесі етіп тағайындау туралы ақпаратты Kaspersky Secure Mobility Management анықтамасынан қараңыз.

Пайдаланушыны ұялы құрылғының иесі етіп тағайындау үшін:

1. Егер сіз виртуалды Басқару серверіне қосылған құрылғының иесін тағайындағыңыз келсе, алдымен виртуалды Басқару серверіне ауысыңыз:

   a. Басты мәзірде, Басқару серверінің ағымдағы атауының оң жағындағы шеврон (›) белгішесін басыңыз.

   b. Қажетті Басқару серверін таңдаңыз.

2. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.

   Пайдаланушылар тізімі ашылады. Егер сіз қазір виртуалды Басқару серверіне қосылған болсаңыз, тізімге ағымдағы виртуалды Басқару сервері мен негізгі Басқару серверінің пайдаланушылары кіреді.

3. Құрылғының иесі ретінде тағайындалуы қажет пайдаланушы есептік жазбасын түртіңіз.

4. Ашылған пайдаланушы сипаттары терезесінде **Құрылғылар** қойыншасын таңдаңыз.

5. **Қосу** түймесін басыңыз.

6. Құрылғылар тізімінен пайдаланушыға тағайындағыңыз келетін құрылғыны таңдаңыз.

7. **OK** түймесін басыңыз.

Таңдалған құрылғы пайдаланушыға тағайындалған құрылғылар тізіміне қосылады.

Сондай-ақ, тағайындағыңыз келетін құрылғы атауын таңдау және **Құрылғы иесін басқару** сілтемесінен өту арқылы, бұл операцияны **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** тобында орындауға болады.

Барлық пайдаланушы үшін екі қадамдық тексеруді конфигурациялау

Бұл сценарий, барлық пайдаланушылар үшін екі қадамдық тексеруді қалай қосу керектігін және екі қадамдық тексеруден пайдаланушы есептік жазбаларын қалай алып тастау керектігін сипаттайды. Егер сіз өзіңіздің есептік жазбаңызды басқа пайдаланушылар үшін қоспас бұрын екі қадамдық тексеруді қоспаған болсаңыз, бағдарлама алдымен сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу терезесін ашады. Бұл сценарий сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қалай қосу керектігін де сипаттайды.

Егер сіз өзіңіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосқан болсаңыз, барлық пайдаланушылар үшін екі қадамдық тексеруді қосуға болады.

Алдын ала талаптар

Бастамас бұрын:

- Басқа пайдаланушылардың есептік жазбаларының қауіпсіздік параметрлерін өзгерту үшін есептік жазбаңызда Жалпы функционал: Пайдаланушы рұқсаттары функционалдық аймағындағы **Нысан ACL параметрлерін өзгерту** құқығы бар екеніне көз жеткізіңіз.
- Басқару серверінің басқа пайдаланушылары өз құрылғыларына аутентификация қолданбасын орнатқанына көз жеткізіңіз.

Кезеңдер

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу келесі кезеңдерден тұрады:

1. **Құрылғыда аутентификация қолданбасы орнатылуда**

   Уақытқа негізделген бір реттік құпиясөз (TOTP) алгоритмін қолдайтын кез келген түпнұсқалықты тексеру қолданбасын орнатуға болады, мысалы:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Яндекс ID
   - Avanpost Authenticator
   - Aladdin 2FA

   Kaspersky Security Center өзіңіз пайдаланғыңыз келетін аутентификация қолданбасын қолдайтынын тексеру үшін, барлық пайдаланушылар немесе белгілі бір пайдаланушы үшін екі факторлы растауды қосыңыз.

   Қадамдардың бірі аутентификация қолданбасы жасаған қауіпсіздік кодын беруді болжайды. Бәрі сәтті болса, Kaspersky Security Center таңдалған түпнұсқалықты тексеру қолданбасын қолдайды.

Басқару серверіне қосылатын сол құрылғыда аутентификация қолданбасын орнату мүлдем ұсынылмайды.

2. **Аутентификация қолданбасының уақытын және Басқару сервері орнатылған құрылғының уақытын синхрондау**

   Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт сыртқы уақыт көздері көмегімен UTC-пен синхрондалғанына көз жеткізіңіз. Әйтпесе, түпнұсқалықты тексеру және екі қадамдық тексеруді белсендіру сәтсіз болуы мүмкін.

3. **Екі қадамдық тексеруді қосу және есептік жазбаңызға құпия кілт алу**

   Нұсқаулар:

   - MMC негізіндегі Басқару консолі үшін: Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу.
   - Kaspersky Security Center Web Console үшін: Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу.

   Есептік жазбаңыз үшін екі қадамдық тексеруді қосқаннан кейін, барлық пайдаланушылар үшін екі қадамдық тексеруді қосуға болады.

4. **Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу**

   Екі қадамдық тексеру қосылған пайдаланушылар оны Басқару серверіне кіру үшін пайдалануы керек.

   Нұсқаулар:

   - MMC негізіндегі Басқару консолі үшін: Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу.
   - Kaspersky Security Center Web Console үшін: Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу.

5. **Қауіпсіздік кодын шығарушының атын өзгерту**

   Аттары ұқсас бірнеше Басқару серверіңіз болса, бәлкім, әртүрлі Басқару серверлерін жақсырақ тану үшін қауіпсіздік кодын шығарушыларын аттарын өзгертуіңізге тура келеді.

   Нұсқаулар:

   - MMC негізіндегі Басқару консолі үшін: Қауіпсіздік кодын шығарушының атын өзгерту.
   - Kaspersky Security Center Web Console үшін: Қауіпсіздік кодын шығарушының атын өзгерту.

6. **Екі қадамдық тексеруді қосуды қажет етпейтін пайдаланушы есептік жазбаларын алып тастау**

   Қажет болса, екі қадамдық тексеруден пайдаланушылардың есептік жазбаларын алып тастаңыз. Есептік жазбалары алынып тасталған пайдаланушыларға Басқару серверіне кіру үшін екі қадамдық тексеруді пайдаланудың қажеті жоқ.

   Нұсқаулар:

   - MMC негізіндегі Басқару консолі үшін: Екі қадамдық тексеруден есептік жазбаларды алып тастау.
   - Kaspersky Security Center Web Console үшін: Екі қадамдық тексеруден есептік жазбаларды алып тастау.

7. **Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді баптау**

   Егер пайдаланушылар екі қадамдық тексеруден алынып тасталмаса және екі қадамдық тексеру әлі есептік жазбалары үшін конфигурацияланбаған болса, олар оны Kaspersky Security Center-ге кірген кезде ашылатын терезеде конфигурациялауы керек. Әйтпесе, олар құқықтарына сәйкес Басқару серверіне қол жеткізе алмайды.

Нұсқаулар:

- MMC негізіндегі Басқару консолі үшін: Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді конфигурациялау.
- Kaspersky Security Center Web Console үшін: Сіздің есептік жазбаңыз үшін екі қадамдық тексеруді конфигурациялау.

Нәтижелер

Бұл сценарийді орындағаннан кейін:

- Сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосулы.
- Жойылған пайдаланушы есептік жазбаларынан басқа Басқару серверінің барлық пайдаланушыларының есептік жазбалары үшін екі қадамдық тексеру кіреді.

Екі қадамдық тексеру туралы

Есептік жазба үшін екі қадамдық тексеру қосылса, Басқару консолі немесе Kaspersky Security Center Web Console веб-консоліне кіру үшін пайдаланушы аты мен құпиясөзден бөлек, бір реттік қауіпсіздік коды қажет. Домендік түпнұсқалық растама қосылса, пайдаланушыға тек бір реттік қауіпсіздік кодын енгізу қажет.

Екі қадамдық тексеруді пайдалану үшін ұялы құрылғыға немесе компьютерге бір реттік қауіпсіздік кодтарын жасайтын аутентификация қолданбасын орнатыңыз. Уақытқа негізделген бір реттік құпиясөз (TOTP) алгоритмін қолдайтын кез келген түпнұсқалықты тексеру қолданбасын пайдалануға болады, мысалы:

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Яндекс ID
- Avanpost Authenticator
- Aladdin 2FA

Kaspersky Security Center өзіңіз пайдаланғыңыз келетін аутентификация қолданбасын қолдайтынын тексеру үшін, барлық пайдаланушылар немесе белгілі бір пайдаланушы үшін екі факторлы растауды қосыңыз.

Қадамдардың бірі аутентификация қолданбасы жасаған қауіпсіздік кодын беруді болжайды. Бәрі сәтті болса, Kaspersky Security Center таңдалған түпнұсқалықты тексеру қолданбасын қолдайды.

Құпия кілтті (немесе QR кодын) сақтап қою және оны қауіпсіз жерде сақтау қатаң ұсынылады. Бұл ұялы құрылғыға қатысу мүмкіндігі жоғалған жағдайда Kaspersky Security Center Web Console серверіне қатынасуды қалпына келтіруге көмектеседі.

Kaspersky Security Center бағдарламасын пайдалануды қамтамасыз ету үшін сіз өзіңіздің есептік жазбаңызға екі қадамдық тексеруді қосып, барлық пайдаланушылар үшін екі қадамдық тексеруді қоса аласыз.

Сіз екі қадамдық тексеруден есептік жазбаларды алып тастай аласыз. Бұл түпнұсқалық растама үшін қауіпсіздік кодын ала алмайтын қызметтік есептік жазбалар үшін қажет болуы мүмкін.

Ережелер және шектеулер

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу және жекелеген пайдаланушылар үшін екі қадамдық тексеруді өшіру мүмкіндігіне ие болу үшін:

- Есептік жазбаңызда Жалпы функционал: Пайдаланушы құқықтары функционалды аймағында **Нысан ACL параметрлерін өзгерту** құқығы бар екеніне көз жеткізіңіз.
- Есептік жазбаңыз үшін екі қадамдық тексеруді қосыңыз.

Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру үшін:

- Есептік жазбаңызда Жалпы функционал: Пайдаланушы құқықтары функционалды аймағында **Нысан ACL параметрлерін өзгерту** құқығы бар екеніне көз жеткізіңіз.
- Екі қадамдық тексеру арқылы Kaspersky Security Center Web Console веб-консолiне кіріңіз.

Егер Kaspersky Security Center 13 немесе одан жоғары нұсқасының Басқару серверіндегі есептік жазба үшін екі қадамдық тексеру қосылған болса, онда пайдаланушы Kaspersky Security Center Web Console серверінің 12, 12.1 немесе 12.2 нұсқаларына кіре алмайды.

Құпия кілтті қайта шығару

Кез келген пайдаланушы екі қадамдық тексеру үшін пайдаланылатын құпия кілтті қайта шығара алады. Пайдаланушы Басқару серверіне қайта шығарылған құпия кілтпен кіргенде, жаңа құпия кілт пайдаланушы есептік жазбасы үшін сақталады. Пайдаланушы жаңа құпия кілтті қате енгізсе, жаңа құпия кілт сақталмайды және ағымдағы құпия кілт жарамды болып қалады.

Қауіпсіздік кодында *шығарушы аты* деп те аталатын идентификатор бар. Қауіпсіздік кодын шығарушының аты аутентификация қолданбасында Басқару сервері идентификаторы ретінде пайдаланылады. Қауіпсіздік кодын шығарушының аты Басқару серверінің атауы сияқты әдепкі бойынша мәнге ие. Қауіпсіздік кодын шығарушының атын өзгерте аласыз. Қауіпсіздік кодын шығарушының атын өзгерткен болсаңыз, жаңа құпия кілтті шығарып, оны аутентификация қолданбасына беру керек.

Есептік жазбаңыз үшін екі қадамдық тексеруді қосу (Web Console)

Сіз өзіңіздің есептік жазбаңыз үшін ғана екі қадамдық тексеруді қоса аласыз.

Есептік жазбаңыз үшін екі қадамдық тексеруді қоспас бұрын, ұялы құрылғыда аутентификация қолданбасы орнатылғанына көз жеткізіңіз. Аутентификация қолданбасында орнатылған уақыт Басқару сервері орнатылған құрылғының уақытымен синхрондалғанына көз жеткізіңіз.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді қосу үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар** бөліміне өтіңіз.
2. Есептік жазбаңыздың атын басыңыз.
3. Ашылған пайдаланушы сипаттары терезесінде **Аутентификация қауіпсіздігі** қойыншасын таңдаңыз.
4. **Аутентификация қауіпсіздігі** қойыншасында:
   a. **Пайдаланушының атын, құпиясөзін және қауіпсіздік кодын сұрау (екі қадамдық тексеру)** параметрін таңдаңыз. **Сақтау** түймесін басыңыз.
   b. Ашылған екі кезеңді тексеру терезесінде **Екі қадамдық тексеруді орнату жолын қараңыз** түймесін басыңыз.
      Аутентификация қолданбасында құпия кілтті енгізіңіз немесе **QR кодын қарау** түймесін басыңыз және бір реттік қауіпсіздік кодын алу үшін мобильді құрылғыдағы аутентификация қолданбасымен QR кодын сканерлеңіз.
   c. Екі қадамдық тексеру терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.
5. **Сақтау** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосулы.

Есептік жазбаңыз үшін екі қадамдық тексеруді қосу (MMC негізінде)

Есептік жазбаңыз үшін екі қадамдық тексеруді қоспас бұрын, ұялы құрылғыда аутентификация қолданбасы орнатылғанына көз жеткізіңіз. Аутентификация қолданбасында орнатылған уақыт Басқару серверінің уақытымен синхрондалғанына көз жеткізіңіз.

Есептік жазба үшін екі қадамдық тексеруді қосу үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.
2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** тақтасындағы **Кеңейтілген** бөліміне, содан соң **Екі қадамдық тексеру** тармағына өтіңіз.
3. **Екі қадамдық тексеру** бөлімінде **Конфигурациялау** түймесін басыңыз.

   > Есептің жазбаңыз үшін екі қадамдық тексеру әлдеқашан қосылған болса, **Баптау** түймесін басу екі қадамдық тексеруді қайта конфигурациялау үшін құпия кілтті қалпына келтіреді.

   Ашылған екі қадамдық тексеру сипаттары терезесінде құпия кілт көрсетіледі.
4. Бір реттік қауіпсіздік кодын алу үшін аутентификация қолданбасына құпия кілтті енгізіңіз. Құпия кілтті қолмен аутентификация қолданбасына енгізуге немесе ұялы құрылғыдағы аутентификация қолданбасымен QR кодын сканерлеуге болады.

5. Аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіңіз, содан кейін екі қадамдық тексеру сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

6. **Қолдану** түймесін басыңыз.

7. **OK** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосулы.

Барлық пайдаланушы үшін міндетті екі қадамдық тексеруді қосу (Web Console)

Есептік жазбаңыздың **Жалпы мүмкіндіктер: пайдаланушы рұқсаттары** функционалды аймағында нысанның ACL параметрлерін өзгерту құқығы болса және екі қадамдық растау көмегімен аутентификациядан өтсеңіз, басқару серверінің барлық пайдаланушысы үшін екі қадамдық растау мүмкіндігін қосуға болады.

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Аутентификация қауіпсіздігі** қойыншасында **барлық пайдаланушылар үшін екі қадамдық тексеруді** қосыңыз.

3. Егер сіз өзіңіздің есептік жазбаңыз үшін екі кезеңді тексеруді қоспаған болсаңыз, бағдарлама сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу терезесін ашады.

   a. Ашылған екі кезеңді тексеру терезесінде **Екі қадамдық тексеруді орнату жолын қараңыз** түймесін басыңыз.

   b. Аутентификатор қолданбасында құпия кілтті қолмен енгізіңіз немесе **QR кодын қарау** түймесін басыңыз және бір реттік қауіпсіздік кодын алу үшін мобильдік құрылғыдағы аутентификатор қолданбасымен QR кодын сканерлеңіз.

   c. Екі қадамдық тексеру терезесінде аутентификатор қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.

Екі кезеңді тексеру барлық пайдаланушылар үшін қосылған. Басқару сервері пайдаланушылары, соның ішінде барлық пайдаланушылар үшін екі қадамдық тексеруді қосқаннан кейін қосылған пайдаланушылар, есептік жазбалары екі қадамдық тексеруден алынып тасталған пайдаланушылардан басқа, өз есептік жазбалары үшін екі қадамдық тексеруді орнатуы керек.

Барлық пайдаланушы үшін екі қадамдық тексеруді қосу (MMC негізінде)

Есептік жазбаңыздың **Жалпы мүмкіндіктер: пайдаланушы рұқсаттары** функционалды аймағында нысанның ACL параметрлерін өзгерту құқығы болса және екі қадамдық растау көмегімен аутентификациядан өтсеңіз, басқару серверінің барлық пайдаланушысы үшін екі қадамдық растау мүмкіндігін қосуға болады.

Барлық пайдаланушылар үшін екі қадамдық тексеруді қосу үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Кеңейтілген** бөлімін, содан соң **Екі қадамдық тексеру** тармағын таңдаңыз.

3. Барлық пайдаланушыларға екі қадамдық тексеруді қосу үшін **Қажетті деп орнату** түймесін басыңыз.

4. Егер сіз өзіңіздің есептік жазбаңыз үшін екі кезеңді тексеруді қоспаған болсаңыз, бағдарлама сіздің есептік жазбаңыз үшін екі қадамдық тексеруді қосу терезесін ашады.

   a. Бір реттік қауіпсіздік кодын алу үшін аутентификация қолданбасына құпия кілтті енгізіңіз. Аутентификация қолданбасында құпия кілтті қолмен енгізіңіз немесе және бір реттік қауіпсіздік кодын алу үшін мобильді құрылғыдағы аутентификация қолданбасымен QR кодын сканерлеңіз.

   b. Аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіңіз, содан кейін екі қадамдық тексеру сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

5. **Екі кезеңді тексеру** бөлімінде **Қолдану** түймесін және **OK** түймесін басыңыз.

Екі кезеңді тексеру барлық пайдаланушылар үшін қосылған. Басқару сервері пайдаланушылары, соның ішінде осы параметрді қосқаннан кейін қосылған пайдаланушылар, есептік жазбалары екі қадамдық тексеруден алынып тасталған пайдаланушылардан басқа, өз есептік жазбалары үшін екі қадамдық тексеруді орнатуы керек.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру (Web Console)

Есептік жазбаңыз үшін, сондай-ақ кез келген басқа пайдаланушының есептік жазбасы үшін екі қадамдық тексеруді өшіруге болады.

Есептік жазбаңыздың **Жалпы функционал: Пайдаланушы құқықтары** функционалдық аймағының Нысанның қолжетімділігін басқару тізімдерін өзгерту құқығы бар болса және сіз екі қадамдық тексеру арқылы түпнұсқалық растаманы орындаған болсаңыз, пайдаланушының басқа есептік жазбасы үшін екі қадамдық тексеруді өшіре аласыз.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар** бөліміне өтіңіз.

2. Екі қадамдық тексеруді өшіргіңіз келетін ішкі пайдаланушы есептік жазбасын басыңыз. Бұл сіздің жеке есептік жазбаңыз немесе кез келген басқа пайдаланушының есептік жазбасы болуы мүмкін.

3. Ашылған пайдаланушы сипаттары терезесінде **Есептік жазба қорғанысы** қойыншасын таңдаңыз.

4. Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіргіңіз келсе, **Есептік жазба қорғанысы** қойыншасында **Тек пайдаланушының аты мен құпиясөзін сұрау** параметрін таңдаңыз.

5. **Сақтау** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру өшірулі.

Екі қадамдық тексеру арқылы Kaspersky Security Center Web Console веб-консоліне кіре алмайтын пайдаланушыға кіру рұқсатын қалпына келтіргіңіз келсе, сол пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіріп, жоғарыда сипатталғандай **Тек пайдаланушының аты мен құпиясөзін сұрау** параметрін таңдаңыз. Осыдан кейін, екі қадамдық тексеруді өшірген пайдаланушы есептік жазбасымен Kaspersky Security Center Web Console веб-консоліне кіріп, тексеруді қайта қосыңыз.

Пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіру (MMC негізінде)

Есептік жазбаңыз үшін екі қадамдық тексеруді өшіру үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.
2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Кеңейтілген** бөлімін, содан соң **Екі қадамдық тексеру** тармағын таңдаңыз.
3. **Екі қадамдық тексеру** бөлімінде **Өшіру** түймесін басыңыз.
4. **Қолдану** түймесін басыңыз.
5. **ОК** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру өшірулі.

Басқа пайдаланушылардың есептік жазбалары үшін екі қадамдық тексеруді өшіруге болады. Бұл қорғаныс, мысалы, пайдаланушы ұялы құрылғыны жоғалтса немесе бұзса қолданылады.

Есептік жазбаңыздың Жалпы функционал: Пайдаланушы құқықтары функционалдық аймағының **Нысанның қолжетімділігін басқару тізімдерін өзгерту** құқығы бар болса және сіз екі қадамдық тексеру арқылы түпнұсқалық растаманы орындаған болсаңыз ғана пайдаланушының басқа есептік жазбасы үшін екі қадамдық тексеруді өшіре аласыз. Сондай-ақ, төменде келтірілген нұсқауларды орындай отырып, сіз өзіңіздің есептік жазбаңыз үшін екі қадамдық тексеруді өшіре аласыз.

Кез келген пайдаланушының есептік жазбасында екі қадамдық тексеруді өшіру үшін:

1. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын ашыңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Қосымша** қалтасына салынған.
2. Қалтаның жұмыс аймағында, екі қадамдық тексеруді өшіргіңіз келетін пайдаланушы есептік жазбасын басыңыз.

   Екі қадамдық тексеру қосылған барлық пайдаланушы есептік жазбалары үшін **2FA қажет етіледі** бағанында **Иә** мәнін белгілеңіз.
3. **Сипаттар: <Пайдаланушы аты>** терезесінде **Екі кезеңді тексеру** бөлімін таңдаңыз.

4. **Екі кезеңді тексеру** бөлімінде келесі параметрлерді таңдаңыз:

   - Таңдалған пайдаланушы есептік жазбасы үшін екі қадамдық тексеруді өшіргіңіз келсе, **Өшіру** түймесін басыңыз.

   - Екі қадамдық тексеруден пайдаланушының осы есептік жазбасын алып тастағыңыз келсе, **Пайдаланушы аутентификацияны тек пайдаланушы аты мен құпиясөзді қолдану арқылы бере алады** параметрін таңдаңыз.

5. **Қолдану** түймесін басыңыз.

6. **OK** түймесін басыңыз.

Пайдаланушы есептік жазбасының екі қадамдық тексеруі өшірулі.

Басқару консоліне екі қадамдық тексеру арқылы кіре алмайтын пайдаланушыға кіру рұқсатын қалпына келтіргіңіз келсе, сол пайдаланушы есептік жазбасы үшін екі сатылы растауды өшіріп, **Екі қадамдық тексеру** бөлімінде, жоғарыда көрсетілгендей, **Пайдаланушы аутентификацияны тек пайдаланушы аты мен құпиясөзді қолдану арқылы бере алады** параметрін таңдаңыз. Осыдан кейін, екі қадамдық тексеруді өшірген пайдаланушы есептік жазбасымен Басқару консоліне кіріп, тексеруді қайта қосыңыз.

Барлық пайдаланушы үшін міндетті екі қадамдық тексеруді өшіру (Web Console)

Сіздің есептік жазбаңыз үшін міндетті екі қадамдық тексеру қосулы болса және сіздің есептік жазбаңызда **Жалпы функционал: Пайдаланушы рұқсаттары** функционалдық аймағының Нысанның ACL тізімдерін өзгерту құқығы болса, сіз барлық пайдаланушылар үшін екі қадамдық тексеруді өшіре аласыз. Егер сіздің есептік жазбаңыз үшін екі қадамдық тексеру қосылмаған болса, оны барлық пайдаланушылар үшін өшірмес бұрын, есептік жазбаңыз үшін екі қадамдық тексеруді қосу керек.

Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер () белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесінің **Аутентификация қауіпсіздігі** қойыншасында **барлық пайдаланушылар үшін екі қадамдық тексеру** қосқышын өшіріңіз.

Барлық пайдаланушылар үшін екі қадамдық тексеру өшірулі. Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру, бұрын екі қадамдық тексеру бөлек қосылған арнайы есептік жазбаларға қолданылмайды.

Барлық пайдаланушы үшін міндетті екі қадамдық тексеруді өшіру (MMC негізінде)

Жалпы функционал: Пайдаланушы рұқсаттары функционалдық аймағының **Нысан ACL параметрлерін өзгерту** құқығыңыз бар болса және сіз міндетті екі қадамдық тексеру арқылы түпнұсқалық растаманы орындаған болсаңыз, Басқару серверінің барлық пайдаланушылары үшін екі қадамдық тексеруді өшіре аласыз.

Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.
2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Кеңейтілген** бөлімін, содан соң **Екі қадамдық тексеру** тармағын таңдаңыз.
3. Барлық пайдаланушыларға екі қадамдық тексеруді өшіру үшін **Міндетті деп орнату** түймесін басыңыз.
4. **Екі кезеңді тексеру** бөлімінде **Қолдану** түймесін басыңыз.
5. **Екі кезеңді тексеру** бөлімінде **OK** түймесін басыңыз.

Барлық пайдаланушылар үшін екі қадамдық тексеру өшірулі. Барлық пайдаланушылар үшін екі қадамдық тексеруді өшіру, бұрын екі қадамдық тексеру бөлек қосылған арнайы есептік жазбаларға қолданылмайды.

Есептік жазбаларды екі қадамдық тексеруден алып тастау (Web Console)

Жалпы функционал: Пайдаланушы рұқсаттары функционалдық аймағының **Нысанның ACL тізімдерін өзгерту** құқығыңыз бар болса, пайдаланушылардың есептік жазбаларын екі қадамдық тексеруден алып тастай аласыз.

Егер пайдаланушы есептік жазбасы барлық пайдаланушылар үшін екі сатылы тексеру тізімінен алынып тасталса, бұл пайдаланушыға екі қадамдық тексеруді пайдаланудың қажеті жоқ.

> Екі қадамдық тексеруден есептік жазбаларды алып тастау түпнұсқалық растама кезінде қауіпсіздік кодын бере алмайтын қызметтік есептік жазбалар үшін қажет болуы мүмкін.

Егер сіз кейбір пайдаланушы есептік жазбаларын екі қадамдық тексеруден алып тастағыңыз келсе:

1. Active Directory есептік жазбаларын алып тастағыңыз келсе, басқару сервері пайдаланушыларының тізімін жаңарту үшін алдымен Microsoft Active Directory домен контроллерінің сауалнамасын жүргізуіңіз керек.
2. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер () белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
3. Екі қадамдық тексеру үшін ерекшеліктер кестесіндегі сипаттар терезесінің **Аутентификация қауіпсіздігі** қойыншасында **Қосу** түймесін басыңыз.
4. Ашылған терезеде:
   a. Жойғыңыз келетін пайдаланушы есептік жазбасын таңдаңыз.
   b. **OK** түймесін басыңыз.

Таңдалған пайдаланушы есептік жазбалары екі қадамдық тексеруден шығарылады.

Есептік жазбаларды екі қадамдық тексеруден алып тастау (MMC негізінде)

Есептік жазбаңызда Жалпы функционал: Пайдаланушы рұқсаттары функционалдық аймағының **Нысан ACL параметрлерін өзгерту** құқығы бар болса, есептік жазбаны екі қадамдық тексеруден алып тастай аласыз.

Егер пайдаланушы есептік жазбасы екі қадамдық тексеруден алынып тасталса, бұл пайдаланушы Басқару консоліне немесе Kaspersky Security Center Web Console серверіне екі қадамдық тексеруді пайдаланбай кіре алады.

Екі қадамдық тексеруден есептік жазбаларды алып тастау түпнұсқалық растама кезінде қауіпсіздік кодын бере алмайтын қызметтік есептік жазбалар үшін қажет болуы мүмкін.

Пайдаланушы есептік жазбасын екі қадамдық тексеруден шығару үшін:

1. Егер сіз Active Directory есептік жазбасын алып тастағыңыз келсе, Басқару сервері пайдаланушыларының тізімін жаңарту үшін Active Directory сауалнамасын орындаңыз.
2. Консоль ағашында **Пайдаланушылардың есептік жазбалары** қалтасын ашыңыз.

   Пайдаланушылардың есептік жазбалары қалтасы әдепкі бойынша **Қосымша** қалтасына салынған.
3. Қалтаның жұмыс аймағында екі қадамдық тексеруден шығарғыңыз келетін пайдаланушы есептік жазбасын басыңыз.
4. **Сипаттар: <Пайдаланушы аты>** терезесінде **Екі кезеңді тексеру** бөлімін таңдаңыз.
5. Ашылған бөлімде **Пайдаланушы аутентификацияны тек пайдаланушы аты мен құпиясөзді қолдану арқылы бере алады** параметрін таңдаңыз.
6. **Екі кезеңді тексеру** бөлімінде **Қолдану** түймесін және **OK** түймесін басыңыз.

Бұл пайдаланушы есептік жазбасы екі қадамдық тексеруден шығарылады. Алынып тасталған есептік жазбаларды пайдаланушы есептік жазбаларының тізімінен тексеруге болады.

Қауіпсіздік кодын шығарушының атын өңдеу (Web Console)

Сізде әртүрлі Басқару серверлері үшін бірнеше идентификаторлар болуы мүмкін (оларды шығарушылар деп те атайды). Қауіпсіздік кодын шығарушының атын өзгертуге болады, мысалы, егер Басқару сервері басқа Басқару сервері үшін ұқсас қауіпсіздік кодын шығарушының атын қолданса. Әдепкі бойынша, қауіпсіздік кодын шығарушының аты Басқару серверінің атымен бірдей.

Қауіпсіздік кодын шығарушының атын өзгерткеннен кейін, жаңа құпия кілтті қайта шығарып, оны аутентификация қолданбасына беру керек.

Қауіпсіздік кодын шығарушының жаңа атын көрсету үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. Ашылған пайдаланушы сипаттары терезесінде **Есептік жазба қорғанысы** қойыншасын таңдаңыз.
3. **Есептік жазба қорғанысы** қойыншасында **Өңдеу** сілтемесінен өтіңіз.

   Қауіпсіздік кодын шығарушыны өзгерту бөлімі ашылады.
4. Қауіпсіздік кодын шығарушының жаңа атын көрсетіңіз.
5. **OK** түймесін басыңыз.

Басқару сервері үшін қауіпсіздік кодын шығарушының жаңа аты көрсетілген.

Қауіпсіздік кодын шығарушының атын өңдеу (MMC негізінде)

Сізде әртүрлі Басқару серверлері үшін бірнеше идентификаторлар болуы мүмкін (оларды шығарушылар деп те атайды). Қауіпсіздік кодын шығарушының атын өзгертуге болады, мысалы, егер Басқару сервері басқа Басқару сервері үшін ұқсас қауіпсіздік кодын шығарушының атын қолданса. Әдепкі бойынша, қауіпсіздік кодын шығарушының аты Басқару серверінің атымен бірдей.

Қауіпсіздік кодын шығарушының атын өзгерткеннен кейін, жаңа құпия кілтті қайта шығарып, оны аутентификация қолданбасына беру керек.

Қауіпсіздік кодын шығарушының жаңа атын көрсету үшін:

1. Kaspersky Security Center консолі шежіресінде тінтуірдің оң жақ түймесімен **Басқару сервері** түйінінің мәтінмәндік мәзірін ашып, **Сипаттар** тармағын таңдаңыз.

2. Басқару сервері сипаттары терезесіндегі **Бөлімдер** панелінде **Кеңейтілген** бөлімін, содан соң **Екі қадамдық тексеру** тармағын таңдаңыз.

3. **Қауіпсіздік кодын шығарушы** өрісінде қауіпсіздік кодын шығарушының жаңа атын көрсетіңіз.

4. **Екі кезеңді тексеру** бөлімінде **Қолдану** түймесін басыңыз.

5. **Екі кезеңді тексеру** бөлімінде **OK** түймесін басыңыз.

Басқару сервері үшін қауіпсіздік кодын шығарушының жаңа аты көрсетілген.

Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурациялау (Web Console)

Екі қадамдық тексеруді қосқаннан кейін, Kaspersky Security Center жүйесіне алғаш рет кірген кезде есептік жазбаңызға арналған екі қадамдық тексеру параметрлері терезесі ашылады.

Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурацияламас бұрын, ұялы құрылғыда аутентификация қолданбасы орнатылғанына көз жеткізіңіз.

Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт сыртқы уақыт көздері көмегімен UTC-пен синхрондалғанына көз жеткізіңіз.

Есептік жазба үшін екі қадамдық тексеруді конфигурациялау үшін:

1. Ұялы құрылғыдағы аутентификация қолданбасын пайдаланып бір реттік қауіпсіздік кодын жасаңыз. Ол үшін келесі әрекеттердің бірін орындаңыз:

   - Құпия кілтті аутентификация қолданбасына қолмен енгізіңіз.

   - **QR кодын қарау** түймесін басып, QR кодын аутентификация қолданбасымен сканерлеңіз.

Қауіпсіздік коды ұялы құрылғыда көрсетіледі.

2. Екі қадамдық тексеру параметрі терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **Тексеру және қолдану** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру конфигурацияланған. Сіздің құқықтарыңызға сәйкес Басқару серверіне қатынасу мүмкіндігі бар.

Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурациялау (MMC негізінде)

Екі қадамдық тексеруді қосқаннан кейін, Kaspersky Security Center жүйесіне алғаш рет кірген кезде есептік жазбаңызға арналған екі қадамдық тексеру параметрлері терезесі ашылады.

Есептік жазбаңыз үшін екі қадамдық тексеруді конфигурацияламас бұрын, ұялы құрылғыда аутентификация қолданбасы орнатылғанына көз жеткізіңіз. Аутентификация қолданбасы бар құрылғыдағы уақыт пен Басқару сервері бар құрылғыдағы уақыт сыртқы уақыт көздері көмегімен UTC-пен синхрондалғанына көз жеткізіңіз.

Есептік жазба үшін екі қадамдық тексеруді конфигурациялау үшін:

1. Ұялы құрылғыдағы аутентификация қолданбасын пайдаланып бір реттік қауіпсіздік кодын жасаңыз. Ол үшін келесі әрекеттердің бірін орындаңыз:

   - Құпия кілтті аутентификация қолданбасына қолмен енгізіңіз.
   - Аутентификация қолданбасымен QR кодын сканерлеңіз.

   Қауіпсіздік коды ұялы құрылғыда көрсетіледі.

2. **Екі қадамдық тексеруді орнату** терезесінде аутентификация қолданбасы жасаған қауіпсіздік кодын көрсетіп, **OK** түймесін басыңыз.

Сіздің есептік жазбаңыз үшін екі қадамдық тексеру конфигурацияланған. Сіздің құқықтарыңызға сәйкес Басқару серверіне қатынасу мүмкіндігі бар.

Жаңа құпия кілтті жасау

Есептік жазбаңызды екі қадамдық тексеру үшін, екі қадамдық тексеру арқылы авторизацияланған болсаңыз ғана жаңа құпия кілт жасай аласыз.

Пайдаланушы есептік жазбасы үшін жаңа құпия кілт жасау үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар** бөліміне өтіңіз.
2. Екі қадамдық тексеру үшін жаңа құпия кілт жасағыңыз келетін пайдаланушы есептік жазбасын басыңыз.
3. Ашылған пайдаланушы сипаттары терезесінде **Есептік жазба қорғанысы** қойыншасын таңдаңыз.
4. **Есептік жазба қорғанысы** қойыншасында **Жаңа құпия кілтті жасау** сілтемесінен өтіңіз.

5. Ашылған екі қадамдық тексеру терезесінде аутентификация қолданбасы жасаған жаңа қауіпсіздік кілтін көрсетіңіз.

6. **Тексеру және қолдану** түймесін басыңыз.

Пайдаланушы үшін жаңа құпия кілт жасалды.

Егер сіз ұялы құрылғыны жоғалтсаңыз, аутентификация қолданбасын басқа ұялы құрылғыға орнатуға және Kaspersky Security Center Web Console сервисіне қатынасуды қалпына келтіру үшін жаңа құпия кілт жасауға болады.

Жаңа пайдаланушыларға өздері үшін екі сатылы растауды орнатуға тыйым салу

Kaspersky Security Center Web Console веб-консоліне кіру қауіпсіздігін одан әрі жақсарту үшін жаңа пайдаланушылардың өздері үшін екі сатылы растауды орнатуына тыйым салуға болады.

Бұл параметр қосылса, жаңа домен әкімшісі сияқты екі сатылы растауды өшірген пайдаланушы өзі үшін екі сатылы растауды орната алмайды. Демек мұндай пайдаланушыны басқару серверінде аутентификациялау мүмкін емес және ол екі қадамдық растау қосылған басқа Kaspersky Security Center әкімшісінің мақұлдауынсыз Kaspersky Security Center Web Console жүйесіне кіре алмайды.

Бұл параметр екі сатылы растау барлық пайдаланушылар үшін қосылған болса қолжетімді болады.

Жаңа пайдаланушылардың өздері үшін екі сатылы растауды орнатуына тыйым салу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. Сипаттар терезесіндегі **Аутентификация қауіпсіздігі** қойындысында **Жаңа пайдаланушыларға екі сатылы растау параметрлерін өз бетінше орнатуға тыйым салу** қосқышын қосыңыз.

Бұл параметр екі сатылы растау ерекшеліктеріне қосылған пайдаланушы есептік жазбаларына әсер етпейді.

Екі сатылы растау өшірілген пайдаланушыға Kaspersky Security Center Web Console консоліне кіру рұқсатын беру үшін **Жаңа пайдаланушыларға екі сатылы растау параметрлерін өз бетінше орнатуға тыйым салу** параметрін уақытша өшіріңіз, пайдаланушыдан екі сатылы растауды қосуды сұраңыз, содан кейін параметрді қайтадан қосыңыз.

Желілік агентті орнатқаннан кейін пайдаланушыны Linux құрылғысының иесі ретінде тағайындау

Пайдаланушыға Linux құрылғысының иесі ретінде тіркелуге рұқсат беру үшін:

1. Kaspersky Security Center Web Console веб-консолінде **Табу және орналастыру → Орналастыру және тағайындау → Орнату пакеттері** бөліміне өтіңіз.

   Орнату пакеттерінің тізімі ашылады.

2. Желілік агенттің орнату пакетін басыңыз.

   Орнату пакеті сипаттары терезесі көрсетіледі.

3. Ашылатын орнату пакетінің сипаттары терезесінде **Параметрлер** → **Кеңейтілген** қойындысына өтіңіз.

4. **Пайдаланушыны құрылғы иесі ретінде тіркеу (тек Linux)** бөлімінде **Желілік агентті орнатқаннан кейін пайдаланушыны тіркеу утилитасын іске қосуға рұқсат беру** параметрін қосып, **Сақтау** түймесін басыңыз.

Пайдаланушыны құрылғы иесі ретінде тіркеуге арналған утилитаны клиент құрылғысындағы пәрмен желісінен іске қосуға болады.

Пайдаланушыны клиент құрылғысында Linux құрылғысының иесі ретінде тіркеу үшін:

1. Клиент құрылғысындағы пәрмен желісінде келесі пәрменді іске қосыңыз:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. Сұралған жағдайда, есептік жазба мен құпиясөзді енгізіңіз.

   Есептік жазба мен құпиясөз жауап файлында немесе Желілік агенттің орнату пакетінде болса, клиент құрылғысындағы пәрмен жолында келесі пәрменді іске қосыңыз:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

Пайдаланушы ішкі қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты болуы керек.

Пайдаланушы Active Directory қауіпсіздік тобының мүшесі болса, есептік жазбада пайдаланушы аты мен домен атауы болуы керек.

Пайдаланушы үшін екі қадамдық тексеру қосылса, сізге қолданбадан уақытша бір реттік құпиясөзді (TOTP) енгізу қажет болады.

Пайдаланушы құрылғы иесі ретінде тіркеледі.

Пайдаланушыларды немесе қауіпсіздік топтарын жою

Ішкі пайдаланушыларды немесе қауіпсіздік топтарын ғана жоюға болады.

Пайдаланушыларды немесе қауіпсіздік топтарын жою:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** немесе **Топтар** қойындысын таңдаңыз.

2. Жойғыңыз келетін пайдаланушы атының немесе қауіпсіздік тобының жанындағы жалаушаны қойыңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **OK** түймесін басыңыз.

   Пайдаланушы немесе қауіпсіздік тобы жойылды.

Пайдаланушы есептік жазбасының құпиясөзін өзгерту

Ағымдағы құпиясөз мерзімі аяқталуға жақын болса немесе оны күштірегіне өзгерткіңіз келсе, жеке есептік жазбаның немесе басқа пайдаланушының есептік жазбасының құпиясөзін өзгерту қажет болуы мүмкін.

Құпиясөз келесі ережелерге сәйкес келуі керек:

- Құпиясөздің ұзындығы 8-ден 256 таңбаға дейін болуы керек.
- Құпиясөзде төмендегі тізімдегі кемінде үш топтың таңбалары болуы керек:
  - Бас әріптер (A-Z)
  - Кіші әріптер (a-z)
  - Сандар (0-9)
  - Арнайы таңбалар (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Құпиясөзде бос орындар, Юникод таңбалары немесе "." таңбасы "@" алдында тұрған кезде "." және "@" тіркесімі болмауы тиіс.

Өз есептік жазбасының құпиясөзін өзгерту

Есептік жазбаңыздың құпиясөзін өзгерту үшін:

1. Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Құпиясөзді өзгерту** опциясын таңдаңыз.
2. Kaspersky Security Center қолданбасына қосылу үшін ағымдағы құпиясөзді енгізіп, жаңа құпиясөзді көрсетіңіз.

   Енгізілген құпиясөзді көру үшін түймесін басыңыз.
3. Пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде "Жалпы функционал: Пайдаланушылар құқықтары" функционалдық аймағында есептік жазбаңыздың деректерін немесе Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар есептік жазба деректерін көрсетіңіз.
4. Алдыңғы қадамда пайдаланған есептік жазба үшін екі сатылы тексеру қосылса, мобильдік құрылғыдағы аутентификация қолданбасы жасаған қауіпсіздік кодын енгізіңіз.

Ішкі пайдаланушының есептік жазбасының құпиясөзін өзгерту

Ішкі пайдаланушы есептік жазбасының құпиясөзін өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Өзгерту қажет болған реттелетін есептік жазбасын таңдаңыз.
3. Ашылатын пайдаланушы сипаттары терезесінде **Жалпы** қойындысындағы **Құпиясөзді өзгерту** түймесін басыңыз.
4. Пайдаланушыны Kaspersky Security Center-ге қосуға арналған жаңа құпиясөз орнатыңыз.

   Енгізілген құпиясөзді көру үшін түймесін басыңыз.

5. Қажет болса, пайдаланушының келесі аутентификациясында құпиясөзді өзгертуге мәжбүрлеу үшін **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрін қосыңыз.

6. Егер пайдаланушы есептік жазбасы рұқсатсыз өзгертуден қорғалған болса, осы есептік жазбаны өзгертуге рұқсатыңыз бар екенін растауыңыз қажет. **Есептік жазба қорғанысы** терезесінде "Жалпы функционал: Пайдаланушылар құқықтары" функционалдық аймағында Нысандарға қол жеткізуді басқару тізімдерін өзгерту құқығы бар есептік жазба деректерін көрсетіңіз.

7. Алдыңғы қадамда пайдаланған есептік жазба үшін екі сатылы тексеру қосылса, мобильдік құрылғыдағы аутентификация қолданбасы жасаған қауіпсіздік кодын енгізіңіз.

Сервер жалаушалары көмегімен құпиясөзді өзгерту параметрлерін конфигурациялау

Klscflag утилитасын пайдаланып, келесі пәрмендер арқылы құпиясөзді өзгертуді реттеуге болады:

- Құпиясөзді ауыстыру кезеңін орнату (`LP_SplPwdChangePeriodDays` жалаушасы).

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>
  ```

  бұл жерде `<айналу_мерзімі>` — пайдаланушы құпиясөзінің мерзімі аяқталатын кезең (күнмен берілген). Ықтимал мәндер: 0–730. Параметр мәні 0 болса, құпиясөзді өзгерту өшірілген.

- Құпиясөзді өзгерту қажеттігі туралы алдыңғы ескерту уақытын конфигурациялау (`LP_SplPwdChangeNotificationHours` жалаушасы)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <ескерту_уақыт>
  ```

  бұл жерде `<ескерту_уақыт>` — пайдаланушы құпиясөзінің мерзімі аяқталатын кезең (сағатпен берілген). Осы уақыт ішінде құпиясөзді өзгертуді сұрайтын хабарландыру көрсетіледі. Ықтимал мәндер: 0–17520. Параметр мәні 0 болса, ескерту уақыты құпиясөзді ауыстыру кезеңінің 25%-ын құрайды.

- **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** параметрі (`LP_SplPwdForceChange` жалаушасы) үшін әдепкі мән нұсқауы.

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <мән>
  ```

  `<мән>` жалаушасының ықтимал мәндері мына жерде:

  `1` — **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** опциясы қосылған.

  `0` — **Пайдаланушы бірінші кірген кезде құпиясөзді өзгертуі керек** опциясы өшірілген.

Жалаушаның ағымдағы мәнін көру үшін келесі пәрменді орындаңыз:

```
klscflag.exe -fget -pv .core/.independent -s KLLIM -n <flag> -t d
```

Мұндағы `<flag>` – `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` немесе `LP_SplPwdForceChange` жалаушасы.

Пайдаланушы рөлін жасау

Пайдаланушы рөлін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Ашылған **Жаңа рөл аты** терезесінде жаңа рөл атауын көрсетіңіз.
4. Өзгерістерді қолдану үшін **OK** түймесін басыңыз.
5. Ашылған терезеде рөл параметрлерін өзгертіңіз:
   - **Жалпы** қойыншасында рөл атауын өзгертіңіз.

     Типтік рөл атауларын өзгерте алмайсыз.
   - **Параметрлер** қойыншасында рөлдің әрекет ету ауқымын, сондай-ақ рөлмен байланысты саясаттар мен саясат профильдерін өзгертіңіз.
   - **Қатынасу құқықтары** қойыншасында Kaspersky бағдарламаларына қатынасу құқықтарын өзгертіңіз.
6. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жасалған рөл пайдаланушы рөлдері тізімінде пайда болады.

Пайдаланушы рөлін өзгерту

Пайдаланушы рөлін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Өзгерту қажет рөлді таңдаңыз.
3. Ашылған терезеде рөл параметрлерін өзгертіңіз:
   - **Жалпы** қойыншасында рөл атауын өзгертіңіз.

     Типтік рөл атауларын өзгерте алмайсыз.
   - **Параметрлер** қойыншасында рөлдің әрекет ету ауқымын, сондай-ақ рөлмен байланысты саясаттар мен саясат профильдерін өзгертіңіз.
   - **Қатынасу құқықтары** қойыншасында Kaspersky бағдарламаларына қатынасу құқықтарын өзгертіңіз.
4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Жаңартылған рөл пайдаланушы рөлдері тізімінде пайда болады.

Пайдаланушы рөлі үшін аймақты өзгерту

Пайдаланушы рөлі ауқымы – бұл пайдаланушылар мен басқару топтарының тіркесімі. Пайдаланушы рөліне қатысты параметрлер тек осы рөл тағайындалған пайдаланушыларға тиесілі құрылғыларға қолданылады және бұл құрылғылар осы рөл тағайындалған топтарға, соның ішінде еншілес топтарға жататын болса ғана қолданылады.

Пайдаланушыларды, қауіпсіздік топтарын және басқару топтарын пайдаланушы рөлінің аймағына қосу үшін келесі тәсілдердің бірін пайдаланыңыз:

1-тәсіл:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** немесе **Топтар** қойындысын таңдаңыз.
2. Рөл аймағына қосу қажет пайдаланушы аттары немесе қауіпсіздік топтарына қарама-қарсы жалаушыларды қойыңыз.
3. **Рөлді тағайындау** түймесін басыңыз.

   Рөлді тағайындау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
4. **Рөлді таңдау** қадамында тағайындау қажет рөлді таңдаңыз.
5. **Ауқымды анықтау** бетінде, рөл аймағына қосу қажет басқару тобын таңдаңыз.
6. Шебер терезесін жабу үшін **Рөлді тағайындау** түймесін басыңыз.

Таңдалған пайдаланушылар, қауіпсіздік топтары және басқару топтары рөл аймағына қосылды.

2-тәсіл:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Аймақты белгілеуді қажет ететін рөлді таңдаңыз.
3. Ашылған рөл сипаттары терезесінде **Параметрлер** қойыншасын таңдаңыз.
4. **Рөл ауқымы** бөлімінде **Қосу** түймесін басыңыз.

   Рөлді тағайындау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
5. **Ауқымды анықтау** бетінде, рөл аймағына қосу қажет басқару тобын таңдаңыз.
6. **Пайдаланушыларды таңдау** бетінде, рөл аймағына қосу қажет пайдаланушылар мен қауіпсіздік топтарын таңдаңыз.
7. Шебер терезесін жабу үшін **Рөлді тағайындау** түймесін басыңыз.
8. Басқару сервері сипаттары терезесін жабу үшін **Жабу** (⨯) түймесін басыңыз.

Таңдалған пайдаланушылар, қауіпсіздік топтары және басқару топтары рөл аймағына қосылды.

3-тәсіл:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Қатынасу құқықтары** қойындысында теңшелетін рөл ауқымын қосқыңыз келетін пайдаланушы немесе қауіпсіздік тобы атының жанындағы құсбелгіні қойып, **Рөлдер** түймесін басыңыз.

   Бір уақытта бірнеше пайдаланушыны немесе қауіпсіздік тобын таңдау мүмкін емес. Бірнеше нысанды таңдасаңыз, **Рөлдер** түймесі өшірулі болады.

3. **Рөлдер** терезесінде тағайындау, қолдану және өзгертулерді сақтағыңыз келетін реттелетін рөлді таңдаңыз.

   Таңдалған пайдаланушылар немесе қауіпсіздік топтары рөлдер ауқымына қосылады.

Пайдаланушы рөлін жою

Пайдаланушы рөлін жою үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Жойғыңыз келетін рөлге қарама-қарсы жалаушаны қойыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **OK** түймесін басыңыз.

Пайдаланушы рөлі жойылады.

Саясат профильдерінің рөлдермен байланысы

Сіз рөлдерді саясат профильдерімен байланыстыра аласыз. Бұл жағдайда, саясат профилі үшін белсендіру ережесі рөлге байланысты анықталады: саясат профилі белгілі бір рөлі бар пайдаланушы үшін белсенді болады.

Мысалы, саясат басқару тобының барлық құрылғылары үшін қалалық навигациялық бағдарламаларды іске қосуға тыйым салады. Қалалық навигация бағдарламалары "Пайдаланушылар" басқару тобында курьер рөлін атқаратын пайдаланушының бір ғана құрылғысының жұмыс істеуі үшін қажет. Бұл жағдайда, бұл құрылғының иесіне "Курьер" рөлін тағайындауға және иелеріне "Курьер" рөлі тағайындалған құрылғыларда қалалық навигация бағдарламаларын қолдануға рұқсат беретін саясат профилін жасауға болады. Барлық басқа саясат параметрлері өзгеріссіз қалады. Тек "Курьер" рөлі бар пайдаланушыларға қалалық навигация бағдарламаларын пайдалануға рұқсат етіледі. Содан кейін, басқа қызметкерге "Курьер" рөлі тағайындалса, онда бұл қызметкер сіздің ұйымыңызға тиесілі құрылғыда қалалық навигациялық бағдарламаларды қолдана алады. Алайда, осы басқару тобының басқа құрылғыларында қалалық навигациялық бағдарламаларды пайдалануға тыйым салынады.

Рөлді саясат профилімен байланыстыру үшін:

1. Бағдарламаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Рөлдер** бөліміне өтіңіз.
2. Саясат профилімен байланыстырылатын рөлді таңдаңыз.

   Жалпы қойыншасында рөл сипаттары терезесі ашылады.

3. **Параметрлер** қойыншасына өтіп, **Саясаттар және профильдер** бөліміне дейін төменге айналдырыңыз.

4. **Өңдеу** түймесін басыңыз.

5. Рөлді осымен байланыстыру үшін:

   - **Қолданыстағы саясат профилімен** – қажетті саясаттың атауының жанындағы (>) белгішесін басыңыз, содан соң рөлді байланыстырғыңыз келетін саясат профилінің жанында жалаушаны қойыңыз.

   - **Жаңа саясат профилі**:

     a. Саясат профилін жасағыңыз келетін саясаттың жанында жалауша қойыңыз.

     b. **Жаңа саясат профилі** түймесін басыңыз.

     c. Жаңа саясат профилінің атауын көрсетіңіз және саясат профилінің параметрлерін конфигурациялаңыз.

     d. **Сақтау** түймесін басыңыз.

     e. Жаңа саясат профилінің жанында жалауша қойыңыз.

6. **Рөлге тағайындау** түймесін басыңыз.

Таңдалған саясат профилі рөлмен байланысып, рөлдің сипаттарында пайда болады. Профиль, иелеріне осы рөл тағайындалған барлық құрылғыларға автоматты түрде қолданылады.

Қосалқы Басқару серверлеріне пайдаланушы рөлдерін тарату

Әдепкі бойынша, негізгі және қосалқы Басқару серверлерінің пайдаланушы рөлдерінің тізімдері тәуелсіз болып саналады. Негізгі Басқару серверінде жасалған пайдаланушы рөлдерін барлық Басқару серверіне автоматты түрде тарату үшін бағдарламаларды орнатуға болады. Пайдаланушы рөлдері қосалқы Басқару серверінен өзінің қосалқы Басқару серверлеріне де таралуы мүмкін.

Пайдаланушы рөлдерін негізгі Басқару серверінен қосалқы Басқару серверлеріне тарату үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **Басқару серверлерінің иерархиясы** бөліміне өтіңіз.

3. **Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу** опциясын қосыңыз, содан кейін **Сақтау** түймесін басыңыз.

Бағдарлама негізгі Басқару сервері пайдаланушыларының рөлдерін қосалқы Басқару серверлеріне көшіреді.

Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу опциясы қосулы және пайдаланушы рөлдері таратылған болса, оларды қосалқы басқару серверінде өңдеу немесе жою мүмкін емес. Негізгі Басқару серверінде рөл жасағанда немесе қолданыстағы рөлді өзгерткенде, өзгерістер автоматты түрде қосалқы Басқару серверлеріне көшіріледі. Негізгі Басқару серверінде пайдаланушы рөлін жойған кезде, бұл рөл қосалқы Басқару серверінде қалады және оны өзгертуге немесе жоюға болады.

Басты серверден қосалқы басқару серверіне таралатын рөлдер жасыл құсбелгілер (✓) арқылы көрсетіледі. Сіз бұл рөлдерді қосалқы Басқару серверінде өзгерте алмайсыз.

Егер рөл негізгі Басқару серверінде жасалса және қосалқы Басқару серверінде бірдей атауы бар рөл болса, жаңа рөл қосалқы Басқару серверіне көшіріледі және оның атына жақшаға нөмір қосылады, мысалы, ~~1, ~~2 (нөмірі кездейсоқ болуы мүмкін).

Рөлдердің тізімін әрі қарай қосалқы Басқару серверлеріне жіберу опциясын өшірсеңіз, барлық пайдаланушы рөлі қосалқы басқару серверлерінде қала береді, бірақ негізгі басқару серверіндегі рөлдерден тәуелсіз болады. Қосалқы Басқару серверлеріндегі рөлдер тәуелсіз болған кезде, оларды өзгертуге немесе жоюға болады.

Есептік жазбаның құпиясөзін ауыстыру

Жергілікті есептік жазбаның құпиясөзін өзгертуге болады, мысалы, пайдаланушы жергілікті есептік жазба құпиясөзін ұмытып қалғанда немесе құпиясөзді кесте бойынша өзгерту үшін.

Құпиясөзді өзгерту пайдаланушы есептік жазбаға кірмеген жағдайда да қолданылады. Сондай-ақ, root жергілікті есептік жазбасы үшін құпиясөзді өзгертуге болады.

Бұл тапсырманы тек Linux басқаруымен жұмыс істейтін құрылғыларда орындауға болады.

Белгілі бір құрылғыларда жергілікті есептік жазба құпиясөзін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** өрісінде **Есептік жазба құпиясөзін өзгерту (тек Linux)** тармағын таңдаңыз.
4. Келесі нұсқалардың бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

Есептік жазба құпиясөзін өзгерту (тек Linux) тапсырмасы көрсетілген құрылғылар үшін жасалады. **Басқару тобына тапсырманы белгілеу** параметрін таңдаған болсаңыз, тапсырма топтық болып саналады.

5. **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғылар таңдауын көрсетіңіз.

   Қолжетімді параметрлер алдыңғы қадамда таңдалған параметрлерге байланысты.

6. **Есептік жазба аты мен жаңа құпиясөзді енгізіңіз** қадамында келесі параметрлерді көрсетіңіз:

   - **Есептік жазбаның атауы** өрісінде құпиясөзді өзгерткіңіз келетін есептік жазбаның атауын енгізіңіз.
   - **Жаңа құпиясөз** жолында алдыңғы өрісте көрсетілген есептік жазба үшін орнатылатын құпиясөзді енгізіңіз.

     Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.
   - Қажет болса, **Бір реттік құпиясөз ретінде орнату (пайдаланушы есептік жазбаға бірінші кіргеннен кейін, құпиясөзді өзгертуі керек)** құсбелгісін қойыңыз.

     - **Бір реттік құпиясөз ретінде орнату (пайдаланушы есептік жазбаға бірінші кіргеннен кейін, құпиясөзді өзгертуі керек)**

       Егер бұл құсбелгі таңдалса, пайдаланушыдан бірінші рет кіргеннен кейін жаңа құпиясөзді өзгерту сұралады.

       Бұл құсбелгі алынып тасталса, пайдаланушыдан бірінші рет кіргеннен кейін жаңа құпиясөзді өзгерту сұралмайды.

       Әдепкі бойынша, жалауша алынып тасталған.

7. Тапсырма жасау және шеберді абу үшін **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

   Жасап болған соң, тапсырма туралы мәліметтерді ашу параметрі қосулы болса, тапсырма параметрлері терезесі ашылады. Бұл терезеде тапсырма параметрлерін тексеруге, оларды өзгертуге немесе қажет болса, тапсырманы іске қосу кестесін конфигурациялауға болады.

8. Тапсырмалар тізімінде жасалған тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

   Немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес тапсырманың іске қосылуын күтіңіз.

Есептік жазба құпиясөзін өзгерту тапсырмасы аяқталғанда, құпиясөз таңдалған құрылғыларда көрсетілген жергілікті есептік жазба үшін өзгертіледі.

Есептік жазба құпиясөзін өзгерту тапсырмаларының дұрыс жұмыс істеуін қамтамасыз ету үшін пайдаланушы құрылғысында SELinux өшірілуі керек.

Жергілікті әкімші құқықтарын кері қайтарып алу

Есептік жазбалар үшін жергілікті әкімші құқықтарын жоюға болады. Бұл пайдаланушы есептік жазбаларын бақылаудың қосымша деңгейін береді. Мысалы, бір реттік тапсырманы орындағаннан кейін жергілікті әкімші құқықтарын жоя аласыз.

Бұл тапсырма іске қосылғанда, көрсетілген жергілікті есептік жазба Желілік агент саясатының параметрлерінде анықталған әкімшілердің жергілікті топтарына жататынын-жатпайтынын тексеру үшін тексеріледі. Әкімшілердің жергілікті топтары тізімін Желілік агент саясатының параметрлерінде конфигурациялай аласыз. Сондай-ақ, артықшылықты пайдаланушы есептік жазбаларының тізімін **Артықшылықтары бар құрылғы пайдаланушылары туралы есеп (тек Linux)** арқылы тексеруге болады.

Бұл тапсырманы тек Linux басқаруымен жұмыс істейтін құрылғыларда орындауға болады.

Белгілі бір құрылғылардағы жергілікті әкімші құқықтарын жою үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. **Тапсырма түрі** өрісінде **Жергілікті әкімші құқықтарын қайтарып алу (тек Linux)** таңдаңыз.
4. Келесі нұсқалардың бірін таңдаңыз:

   - **Басқару тобына тапсырманы белгілеу**

     Тапсырма бұрын жасалған басқару тобына кіретін құрылғыларға тағайындалады. Бар топтардың бірін көрсетуге немесе жаңа топ құруға болады.

     Мысалы, хабар белгілі бір басқару тобындағы құрылғыларға арналған болса, пайдаланушыларға хабар жіберу тапсырмасын іске қосу үшін осы параметрді пайдалануға болады.

     Тапсырма Басқару тобына тағайындалса, **Қауіпсіздік** қойындысы тапсырма сипаттары терезесінде көрсетілмейді, себебі топтық тапсырмалар олар тиесілі болып саналатын қауіпсіздік топтарының параметрлеріне бағынады.

   - **Құрылғының мекенжайларын қолмен белгілеу немесе тізімнен импорттау**

     Сіз NetBIOS атауларын, DNS атауларын, IP мекенжайларын, сондай-ақ тапсырманы тағайындауды қажет ететін құрылғылардың IP мекенжайы ауқымдарын белгілей аласыз.

     Бұл параметрді белгіленген ішкі желі үшін тапсырманы орындау үшін пайдалануға болады. Мысалы, сіз бухгалтерлердің құрылғыларына белгілі бір бағдарламаны орната аласыз немесе вирус жұқтыруы мүмкін ішкі желідегі құрылғыларды тексере аласыз.

   - **Құрылғы таңдауына тапсырманы белгілеу**

     Тапсырма құрылғы таңдауларына кіретін құрылғыларға тағайындалады. Қолданыстағы таңдаулардың бірін көрсетуге болады.

     Мысалы, операциялық жүйенің белгілі бір нұсқасы бар құрылғыларда тапсырманы іске қосу үшін осы параметрді пайдалануға болады.

   Көрсетілген құрылғылар үшін тапсырма жасалады: *Жергілікті әкімші құқықтарын кері қайтарып алу (тек Linux үшін)*. **Басқару тобына тапсырманы белгілеу** параметрін таңдаған болсаңыз, тапсырма топтық болып саналады.
5. **Тапсырма ауқымы** қадамында басқару тобын, нақты мекенжайлары бар құрылғыларды немесе құрылғылар таңдауын көрсетіңіз.

   Қолжетімді параметрлер алдыңғы қадамда таңдалған параметрлерге байланысты.

6. Шебердің осы қадамында келесі параметрлерді көрсетіңіз:

   - **Жұмыс режимі** параметрлер тобында жұмыс режимін таңдаңыз:

     - **Берілген есептік жазбалардан жергілікті әкімші құқықтарын қайтарып алу**

       Бұл параметр таңдалса, жергілікті әкімші құқықтары көрсетілген жергілікті есептік жазбалар үшін жойылады.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **Жергілікті әкімші құқықтарын қайтарып алудан берілген есептік жазбаларды шығару**

       Бұл параметр таңдалса, жергілікті әкімші құқықтары көрсетілгендерден басқа барлық жергілікті есептік жазбалар үшін жойылады.

       Әдепкі бойынша нұсқа таңдалмаған.

   - Жергілікті есептік жазбаларды көрсетіңіз:

     - **Қосу** түймесін басыңыз.

     - Ашылған терезеде келесі әрекеттердің бірін орындаңыз:

       - **Есептік жазбаның атауы** өрісінде жергілікті есептік жазбаңыздың атауын көрсетіңіз.

       - **Есептік жазба әрекеті** параметрлер тобында (**Берілген есептік жазбалардан жергілікті әкімші құқықтарын қайтарып алу** параметрі таңдалған жағдайда қолжетімді) әрекетті таңдаңыз.

       - **Есептік жазбаны сақтау**

         Бұл параметр таңдалса, жергілікті әкімші құқықтары жойылғаннан кейін жергілікті есептік жазба жойылмайды.

         Әдепкі бойынша, осы нұсқа таңдалған.

       - **Есептік жазбаны жою**

         Бұл параметр таңдалса, жергілікті есептік жазба жергілікті әкімші құқықтарының бар-жоғына қарамастан жойылады.

         Әдепкі бойынша нұсқа таңдалмаған.

7. Тапсырма жасау және шеберді абу үшін **Тапсырманы жасауды аяқтау** қадамында **Аяқтау** түймесін басыңыз.

   Жасап болған соң, тапсырма туралы мәліметтерді ашу параметрі қосулы болса, тапсырма параметрлері терезесі ашылады. Бұл терезеде тапсырма параметрлерін тексеруге, оларды өзгертуге немесе қажет болса, тапсырманы іске қосу кестесін конфигурациялауға болады.

8. Тапсырмалар тізімінде жасалған тапсырманы таңдап, **Іске қосу** түймесін басыңыз.

   Немесе тапсырма параметрлерінде көрсетілген кестеге сәйкес тапсырманың іске қосылуын күтіңіз.

Тапсырма аяқталғаннан кейін таңдалған құрылғылардағы көрсетілген жергілікті есептік жазбалар үшін жергілікті әкімші құқықтары жойылады.

Нысанды тексерумен жұмыс

Бұл бөлімде нысандарды тексерумен жұмыс істеу туралы ақпарат бар. Kaspersky Security Center нысандардың өзгерістерін бақылауға мүмкіндік береді. Нысанның өзгерістерін сақтаған сайын, *тексеру* жасалады. Әр тексерудің өзі нөмірі бар.

Тексерулермен жұмысты қолдайтын бағдарлама нысандары:

- Басқару серверінің қасиеттері
- Саясаттар
- Тапсырмалар
- Басқару топтары
- Пайдаланушы есептік жазбалары
- Орнату пакеттері

Нысандарды тексерумен келесі әрекеттерді орындауыңызға болады:

- таңдалған тексерісті қарау (саясаттар үшін ғана қолжетімді);
- нысанның өзгерістерін таңдалған тексеруге шегіндіру;
- тексерістерді JSON файлы ретінде сақтау (тек саясаттар үшін қолжетімді).

Тексерулермен жұмыс істеуді қолдайтын нысандардың сипаттары терезесінде **Тексерістер журналы** бөлімінде келесі ақпаратпен бірге нысанды тексеру тізімі көрсетіледі:

- **Тексеру** – нысанды тексеру нөмірі.
- **Уақыт** – нысанды өзгерту күні мен уақыты.
- **Пайдаланушы** – нысанды өзгерткен пайдаланушы атауы.
- **Пайдаланушы құрылғысының IP мекенжайы** – нысан өзгертілген құрылғының IP-мекенжайы.
- **Web Console консольдің IP мекенжайы** – нысан өзгертілген Kaspersky Security Center Web Console қолданбасының IP-мекенжайы.
- **Әрекет** – нысанмен орындалған әрекет.
- **Сипаттама** – нысан параметрлерінің өзгерістерін тексеру сипаттамасы.

  Әдепкі бойынша, нысанды тексеру сипаттамасы толтырылмаған. Тексеру сипаттамасын қосу үшін қажетті тексеруді таңдап, **Сипаттаманы өңдеу** түймесін басыңыз. Ашылған терезеде тексеру сипаттамасы мәтінін енгізіңіз.

Нысанның өзгерістерін алдыңғы тексеруге шегіндіру

Қажет болса, нысанның өзгерістерін шегіндіруге болады. Мысалы, саясат параметрлерін белгілі бір күндегі күйге кері қайтару қажет болып қалуы мүмкін.

Нысан өзгерістерін шегіндіру үшін:

1. Нысан сипаттары терезесінде **Тексерістер журналы** қойыншасына өтіңіз.
2. Нысанды тексеру тізімінде, өзгерістерін шегіндіру қажет болған тексеруді таңдаңыз.
3. **Шегіндіру** түймесін басыңыз.
4. Операцияны растау үшін **OK** түймесін басыңыз.

   Таңдалған тексеруге шегіндіру орын алады. Нысанды тексеру тізімінде орындалған әрекет туралы жазба көрсетіледі. Тексеру сипаттамасында, нысанды қайтарған тексеру нөмірі туралы ақпарат көрсетіледі.

Шегіндіру операциясы тек саясат пен тапсырмалар үшін қолжетімді.

Тексерудің сипаттамасын қосу

Kaspersky Security Center нысандардың өзгерістерін бақылауға мүмкіндік береді. Нысанның өзгерістерін сақтаған сайын, тексеру жасалады. Әр тексерудің өзі нөмірі бар.

Алдағыда тізімде қажетті тексеруді оңай тауып алу үшін тексеру сипаттамасын қосуға болады.

Тексеру сипаттамасын қосу үшін:

1. Нысан сипаттары терезесінде **Тексерістер журналы** қойындысына өтіңіз.
2. Нысанды тексеру тізімінде, сипаттамасын қосу қажет болған тексеруді таңдаңыз.
3. **Сипаттаманы өңдеу** түймесін басыңыз.

   Сипаттама терезесі ашылады.
4. **Сипаттама** терезесінде тексеру сипаттамасы мәтінін енгізіңіз.

   Әдепкі бойынша, нысанды тексеру сипаттамасы толтырылмаған.
5. Тексеру сипаттамасын сақтаңыз.

Нысанды тексеру үшін сипаттама қосылды.

Саясаттың нұсқасын қарау және сақтау

Kaspersky Security Center қолданбасы белгілі бір кезеңде саясатқа қандай өзгерістер енгізілгенін көруге және осы өзгерістер туралы ақпаратты файлда сақтауға мүмкіндік береді.

Тиісті веб-басқару плагині бұл функцияны қолдайтын болса, саясаттың тексерісін қарау және сақтау қолжетімді болады.

Саясат тексерісін қарау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Көргіңіз келетін саясат тексерісін нұқыңыз және **Тексерістер журналы** бөліміне өтіңіз.
3. Саясат тексерістерінің тізімінде көргіңіз келетін тексеріс нөмірін басыңыз.

   Тексеріс өлшемі 10 МБ-тан асса, оны Kaspersky Security Center Web Console веб-консолі арқылы қарау мүмкін емес. Сізге таңдалған тексерісті JSON файлына сақтау ұсынылады.

   Тексеріс өлшемі 10 МБ-тан аз болса, таңдалған саясат тексерісінің параметрлерімен HTML пішіміндегі есеп көрсетіледі. Есеп қалқымалы терезеде пайда болғандықтан, браузеріңізде қалқымалы терезелерге рұқсат етілгеніне көз жеткізіңіз.

Саясаттың тексерісін JSON файлына сақтау үшін,

Саясат тексерістері тізімінде сақтағыңыз келетін тексерісті таңдап, **Файлға сақталуда** түймесін басыңыз.

Тексеріс JSON файлында сақталады.

Нысандарды жою

Бұл бөлімде нысандарды жою туралы ақпарат берілген.

Сіз келесі нысандарды жоя аласыз:

- Саясаттар
- Тапсырмалар
- Орнату пакеттері
- Виртуалды Басқару серверлері
- Пайдаланушылар
- Қауіпсіздік топтары
- Басқару топтары

Нысанды жою үшін:

1. Kaspersky Security Center Web Console қажетті бөлімін ашып, нысанды таңдаңыз.
2. Құралдар тақтасындағы **Жою** түймесін басыңыз.
3. Пайда болған терезеде таңдауыңызды растау үшін **OK** түймесін басыңыз.

Таңдалған нысан жойылды.

Сіз нысанды жойған кезде, бұл туралы ақпарат дерекқорға жазылады. Жойылған нысандардың ақпаратын сақтау мерзімі, нысанды тексеруді сақтау мерзімімен бірдей (ұсынылатын мерзімі 90 күн). Құқықтардың **Жойылған нысандар** аймағында **Өзгерту** рұқсатыңыз болса ғана, сақтау орнының шартын өзгертуге болады.

Клиенттік құрылғыларды жою туралы

Басқарылатын құрылғы басқару тобынан жойылғанда, бағдарлама құрылғыны Тағайындалмаған құрылғылар тобына жылжытады. Құрылғы жойылғаннан кейін, Kaspersky орнатылған қолданбалары – Желілік агент және Kaspersky Endpoint Security сияқты қауіпсіздік бағдарламасы құрылғыда қалады.

Kaspersky Security Center келесі ережелерге сәйкес Тағайындалмаған құрылғылар тобындағы құрылғыларды өңдейді:

- Құрылғыны жылжыту ережелерін конфигурациялаған болсаңыз және құрылғы жылжыту ережесінің шарттарына сай болса, құрылғы ережеге сәйкес автоматты түрде басқару тобына жылжытылады.
- Құрылғы Тағайындалмаған құрылғылар тобында сақталады және құрылғыны сақтау ережелеріне сәйкес топтан автоматты түрде жойылады.

  Құрылғыны сақтау ережелері, бір немесе бірнеше дискілері толық дискілік шифрлау арқылы шифрланған құрылғыларға әсер етпейді. Мұндай құрылғылар автоматты түрде жойылмайды – оларды тек қолмен жоюға болады. Шифрланған қатты дискісі бар құрылғыны жою қажет болса, алдымен дискінің шифрын шешіп, содан кейін құрылғыны алып тастаңыз.

  > Шифрланған қатты дискісі бар құрылғыны алып тастаған кезде, дискінің шифрын шешуге қажетті деректер де жойылады. Егер сіз осындай құрылғыларды (**Тағайындалмаған құрылғылар** тобынан немесе **Басқарылатын құрылғылар** тобынан) жойған кезде ашылатын растау терезесінде **Тәуекелді түсінемін және таңдалған құрылғыларды жойғым келеді** құсбелгісін қойсаңыз, бұл сіздің деректердің кейінірек жойылатынын білетініңізді білдіреді.

  Бұл жағдайда, дискінің шифрын ашу үшін келесі шарттар орындалуы керек:

  - Дискінің шифрын шешуге қажетті деректерді қалпына келтіру үшін құрылғы Басқару серверіне қайта қосылады.
  - Құрылғының пайдаланушысы шифрды шешу құпиясөзін есте сақтайды.
  - Құрылғыда Kaspersky Endpoint Security for Windows сияқты дискіні шифрлау үшін пайдаланылған қауіпсіздік бағдарламасы орнатылған.

Егер диск Kaspersky Disk Encryption технологиясы арқылы шифрланған болса, FDERT Restore утилитасын пайдаланып деректерді қалпына келтіруге де болады.

VDI жүйесінде шифрланған дискілері бар құрылғы болса, құрылғыны жойғаннан кейін шифрланған дискідегі ақпарат жойылады.

Құрылғыны Тағайындалмаған құрылғылар тобынан қолмен жойған кезде, бағдарлама құрылғыны тізімнен жояды. Құрылғы жойылғаннан кейін, Kaspersky орнатылған бағдарламалары (бар болса) құрылғыда қалады. Содан кейін, құрылғы әлі де Басқару серверіне көрініп тұрса және сіз тұрақты желі сұрауын конфигурациялаған болсаңыз, Kaspersky Security Center Linux желі сауалнамалары кезінде құрылғыны анықтайды және оны Тағайындалмаған құрылғылар тобына қайта қосады. Сондықтан, егер ол Басқару серверіне көрінбейтін болса ғана құрылғыны қолмен алып тастаған жөн.

Kaspersky Security Network (KSN)

Бұл бөлімде Kaspersky Security Network (KSN) онлайн-қызметтері инфрақұрылымын қолдану тәсілі сипатталған. KSN туралы ақпарат, сондай-ақ KSN қосу, KSN бағдарламасына қатынасуды конфигурациялау, KSN прокси-серверін пайдалану статистикасын қарау бойынша нұсқаулар берілген.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

KSN туралы

Kaspersky Security Network (KSN) – файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы Kaspersky жедел білім базасына қатынасуды ұсынатын онлайн-қызметтер инфрақұрылымы. Kaspersky Security Network деректерін пайдалану Kaspersky бағдарламаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады. KSN қолданбасы Kaspersky беделдік дерекқорларынан басқарылатын құрылғыларға орнатылған қолданбалар туралы ақпаратты алуға мүмкіндік береді.

Kaspersky Security Center қолданбасы келесі инфрақұрылымдық шешімдерін қолдайды:

- *KSN* – Kaspersky Security Network қолданбасымен ақпарат алмасуға мүмкіндік беретін шешім. KSN бағдарламасына қатыса отырып, сіз автоматты режимде Kaspersky ұйымына Kaspersky Security Center басқаратын клиент құрылғыларына орнатылған Kaspersky бағдарламаларының жұмысы туралы ақпарат беруге келісесіз. Ақпаратты беру, конфигурацияланған KSN бағдарламасына қатынасу параметрлеріне сәйкес орындалады. Kaspersky мамандары алынған ақпаратты қосымша талдап, оны Kaspersky Security Network беделдік және статистикалық дерекқорларына қосады. Kaspersky Security Center бағдарламасы осы шешімді әдепкі бойынша қолданады.

- *Kaspersky Private Security Network (KPSN)* – бұл Kaspersky қолданбалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан жаһандық KSN қолданбасына деректерді жібермей, Kaspersky Security Network дерекқорларына және басқа да статистикалық деректерге қол жеткізуді қамтамасыз ететін шешім. KPSN келесі себептердің бірі бойынша Kaspersky Security Network бағдарламасына қатыса алмайтын ұйымдарға арналған:

  - Пайдаланушы құрылғылары интернетке қосылмаған.

  - Кез келген деректерді елден немесе корпоративтік желіден (LAN) тыс жерге жіберуге заңмен немесе корпоративті қауіпсіздік саясаттарымен тыйым салынады.

  Басқару сервері терезесінің **KSN-прокси параметрлері** бөлімінде Kaspersky Private Security Network қатынасу параметрлерін конфигурациялай аласыз.

Бағдарлама, бағдарламаны жылдам іске қосу шеберінің жұмысы барысында KSN бағдарламасына қосылуға ұсынады. Қолданбаны пайдаланған кезде, KSN-ді пайдалануды кез келген уақытта бастауға не тоқтатуға болады.

Сіз KSN бағдарламасын KSN қосу кезінде оқитын және қабылдайтын KSN мәлімдемесіне сай қолданасыз. KSN мәлімдемесі жаңартылған болса, ол басқару серверін алдыңғы нұсқасынан жаңарту кезінде көрсетіледі. Сіз жаңартылған KSN мәлімдемесін қабылдауға немесе қабылдамауға болады. Оны қабылдамасаңыз, сіз бұған дейін қабылдаған KSN мәлімдемесінің алдыңғы нұсқасына сәйкес KSN бағдарламасын қолдануды жалғастырасыз.

KSN қосулы болған кезде, Kaspersky Security Center бағдарламасы KSN серверлерінің қолжетімді болуын тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Бұл, қауіпсіздік деңгейіне басқарылатын құрылғылар үшін қолдау көрсетілетіндігіне көз жеткізу үшін керек.

Басқару сервері басқаратын клиент құрылғылары KSN бағдарламасымен KSN прокси-серверінің көмегімен өзара әрекеттеседі. KSN прокси-сервері қызметі келесі мүмкіндіктерді ұсынады:

- Клиент құрылғылары, тіпті интернетке тікелей қатынасу мүмкіндігі болмаса да, KSN бағдарламасына сұраулар жасай алады, KSN бағдарламасынан ақпарат ала алады және KSN бағдарламасына ақпаратты жібере алады.

- KSN прокси-сервері өңделген деректерді кэштей отырып сыртқы желіге арнаға түсетін жүктемені азайтады және клиент құрылғысының сұралған ақпаратты алуын тездетеді.

Сіз KSN прокси-сервері параметрлерін Басқару сервері сипаттары терезесінің **KSN-прокси параметрлері** бөлімінде конфигурациялай аласыз.

KSN бағдарламасына қатынасуды конфигурациялау

Kaspersky Security Network (KSN) бағдарламасына Басқару серверінен және тарату нүктесінен қатынасуды белгілеуге болады.

Басқару серверінің KSN бағдарламасына қатынасуын конфигурациялау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN-прокси параметрлері** бөлімін таңдаңыз.

3. Қосқышты **Басқару серверіндегі KSN Проксиді қосу Қосулы** күйіне ауыстырыңыз.

   Бұл параметр қосылса, KSN прокси-сервері Kaspersky Security Center компоненттері мен Kaspersky қолданбаларының жұмыс тиімділігін арттыру үшін деректерді KSN-ге жібереді. KSN-де клиент құрылғыларынан деректерді беру клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security саясатымен реттеледі. Қосқыш өшірілсе, басқару серверінен және клиенттік құрылғылардан Kaspersky Security Center арқылы KSN қолданбасына деректер берілмейді. Бұл ретте, клиент құрылғылары өздерінің параметрлеріне сәйкес деректерді KSN бағдарламасына тікелей (Kaspersky Security Center арқылы емес) жібере алады. Клиент құрылғыларында жұмыс істейтін Kaspersky Endpoint Security саясаты осы құрылғылардың қандай деректерін тікелей (Kaspersky Security Center арқылы емес) KSN бағдарламасына жіберетінін анықтайды.

4. Қосқышты **Kaspersky Security Network пайдалану Қосулы** күйіне ауыстырыңыз.

   Егер параметр қосулы болса, клиент құрылғылары патчтарды орнату нәтижелерін Kaspersky бағдарламасына жібереді. Бұл параметрді қосқан кезде KSN мәлімдемесі шарттарын оқып, қабылдағаныңызға көз жеткізіңіз.

   KPSN пайдалансаңыз, қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытыңыз және KPSN параметрлерін (pkcs7 және pem кеңейтімдері бар файлдар) жүктеп алу үшін **KSN-прокси параметрлері бар файлды таңдау** түймесін басыңыз. Параметрлер жүктелгеннен кейін, интерфейсте провайдердің атауы, провайдердің контактілері және KPSN параметрлері бар файл жасалған күн көрсетіледі.

   > KSN қосылған кезде, KSN сұрауларын тікелей KSN бұлтты қызметіне жіберуге конфигурацияланған тарату нүктелеріне назар аударыңыз. Желілік агенттің 11 (немесе одан бұрынғы) нұсқасы орнатылған тарату нүктелері KSN бұлтты қызметіне тікелей қатынаса алмайды. KSN сұрауларын KPSN-ге жіберу үшін тарату нүктелерін қайта реттеу мақсатында әр тарату нүктесіне **KSN сұрауын Басқару серверіне қайта жіберу** параметрін қосыңыз. Бұл параметрді тарату нүктесінің немесе Желілік агент саясатының сипаттарында қосуға болады.

   Қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытқанда, KPSN туралы толық ақпарат бар хабар пайда болады.

   KPSN келесі Kaspersky қолданбаларына қолдау көрсетеді:

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux

- Kaspersky Security for Virtualization 3.0 Агентсіз қорғаныс Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Жеңіл агент

KPSN қолданбасын Kaspersky Security Center жүйесіне қоссаңыз, бұл қолданбалар KPSN қолдауы туралы ақпарат алады. Қолданба сипаттары терезесіндегі **Кеңейтілген қорғаныс** бөлімінің **Kaspersky Security Network** бөлімшесінде KSN: KSN немесе KPSN жеткізушісі көрсетіледі.

KPSN қолданбасымен жұмыс істеу үшін Kaspersky Security for Virtualization 3.0, агентсіз қорғаныс Service Pack 2 нұсқасынан төмен немесе Kaspersky Security for Virtualization 3.0 Service Pack 1, жеңіл агент нұсқасынан төмен қолданбаларды пайдалансаңыз, KPSN қолданбасын пайдалану конфигурацияланбаған қосалқы басқару серверлерін пайдалану ұсынылады.

KSN-прокси параметрлері бөліміндегі басқару сервері сипаттары терезесінде KSN орнатылмаған болса, Kaspersky Security Center жүйесі Kaspersky Security Network статистикасын жібермейді.

5. Прокси-сервер параметрлері басқару сервері сипаттарында орнатылса, бірақ желі архитектурасы KPSN-ді тікелей пайдалануды талап ететін болса, **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу** жалаушасын қойыңыз. Әйтпесе, басқарылатын қолданбадан сұрау KPSN қолданбасына берілмейді.

6. Басқару серверін KSN прокси-сервері қызметіне қосу параметрлерін конфигурациялаңыз:

   - **Қосылым параметрлері** блогында, **TCP порты** енгізу өрісінде, KSN прокси-серверіне қосылу орындалатын TCP порты нөмірін көрсетіңіз. Әдепкі бойынша, KSN прокси-серверіне қосылу 13111-порт арқылы жүзеге асырылады.
   - Басқару серверін UDP порты арқылы KSN прокси-серверіне қосу үшін **UDP портын пайдалану** параметрін таңдап, **UDP порты** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі, TCP порты қолданылады. Егер параметр қосулы болса, әдепкі бойынша KSN прокси-серверіне қосылу 15111 санды UDP порты арқылы жүзеге асырылады.
   - Басқару серверін HTTPS порты арқылы KSN прокси-серверіне қосу үшін **HTTPS пайдалану** параметрін таңдап, **Порт арқылы HTTPS** өрісінде порт нөмірін көрсетіңіз. Әдепкі бойынша, параметр өшірулі, TCP порты қолданылады. Егер параметр қосулы болса, әдепкі бойынша KSN прокси-серверіне қосылу 17111 санды HTTPS порты арқылы жүзеге асырылады.

7. Қосқышты **Қосалқы Басқару серверлерін KSN желісіне негізгі Басқару сервері арқылы қосу Қосулы** күйіне ауыстырыңыз.

   Егер бұл параметр қосулы болса, қосалқы Басқару серверлері негізгі Басқару серверін KSN прокси-сервері ретінде пайдаланады. Егер бұл параметр өшірулі болса, қосалқы Басқару серверлері KSN бағдарламасына өздігінен қосылады. Бұл жағдайда, басқарылатын құрылғылар қосалқы Басқару серверлерін KSN прокси-серверлері ретінде пайдаланады.

   Егер **KSN-прокси параметрлері** бөліміндегі қосалқы Басқару серверлерінің сипаттарында қосқыш дәл солай **Басқару серверіндегі KSN Проксиді қосу Қосулы** күйіне ауыстырылса, қосалқы Басқару серверлері негізгі Басқару серверін прокси-сервер ретінде пайдаланады.

8. **Сақтау** түймесін басыңыз.

Нәтижесінде, KSN бағдарламасына қатынасу параметрлері сақталады.

Сондай-ақ, KSN бағдарламасына тарату нүктесі жағынан қатынасуды конфигурациялауға болады, мысалы, Басқару серверіне жүктемені азайту қажет болса. KSN прокси-серверінің рөлін атқаратын тарату нүктесі, Басқару серверін айналып өтіп, басқарылатын құрылғылардан келетін KSN сұрауларын тікелей Kaspersky бағдарламасына жібереді.

Тарату нүктесінің Kaspersky Security Network (KSN) бағдарламасына қатынасуын конфигурациялау үшін:

1. Тарату нүктесі қолмен тағайындалғанына көз жеткізіңіз.
2. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
3. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.
4. Оның сипаттары терезесін ашу үшін тарату нүктесінің атын басыңыз.
5. Тарату нүктесі сипаттары терезесінде, **KSN Проксиі** бөлімінде **Тарату нүктесі тарапынан KSN проксиін қосу** параметрі мен **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру** параметрін қосыңыз.
6. **ОК** түймесін басыңыз.

Тарату нүктесі KSN прокси-серверінің рөлін атқарады.

KSN қолданысын қосу және өшіру

KSN қолданысын қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. **Жалпы** қойыншасында **KSN-прокси параметрлері** бөлімін таңдаңыз.
3. Қосқышты **Басқару серверіндегі KSN Проксиді қосу Қосулы** күйіне ауыстырыңыз.

KSN прокси-сервері қосылды және Kaspersky Security Center компоненттері мен Kaspersky қолданбаларының жұмыс тиімділігін арттыру үшін деректерді KSN-ге жібереді.

1. Қолданылатын KSN инфрақұрылымының шешіміне байланысты сәйкес қосқыштарды қосыңыз.
   - Глобалды KSN қолдансаңыз, қосқышты **Kaspersky Security Network пайдалану Қосулы** күйіне ауыстырыңыз.

     Енді KSN-ге деректер жіберу қолжетімді. Бұл параметрді қоссаңыз, KSN мәлімдемесін оқып, оның шарттарын қабылдауыңыз қажет.

- KPSN пайдалансаңыз, қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытыңыз және KPSN параметрлерін (pkcs7 және pem кеңейтімдері бар файлдар) жүктеп алу үшін **KSN-прокси параметрлері бар файлды таңдау** түймесін басыңыз. Параметрлер жүктелгеннен кейін, интерфейсте провайдердің атауы, провайдердің контактілері және KPSN параметрлері бар файл жасалған күн көрсетіледі.

  Қосқышты **Kaspersky Private Security Network пайдалану Қосулы** күйіне жылжытқанда, KPSN туралы толық ақпараты бар хабар пайда болады.

2. **Сақтау** түймесін басыңыз.

KSN қолданысын өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN-прокси параметрлері** бөлімін таңдаңыз.

3. KSN прокси-сервері қызметін өшіру үшін қосқышты **Басқару серверіндегі KSN Проксиді қосу Өшірулі** күйіне ауыстырыңыз.

4. **Сақтау** түймесін басыңыз.

Қабылданған KSN мәлімдемесін қарау

Kaspersky Security Network (KSN) қосқан кезде сіз KSN мәлімдемесін оқып, қабылдауыңыз керек. Сіз қабылданған KSN мәлімдемесін кез келген уақытта көре аласыз.

Қабылданған KSN мәлімдемесін қарап шығу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN-прокси параметрлері** бөлімін таңдаңыз.

3. **Kaspersky Security Network мәлімдемесін қарау** сілтемесінен өтіңіз.

Ашылған терезеде сіз қабылданған KSN мәлімдемесінің мәтінін көре аласыз.

Жаңартылған KSN мәлімдемесін қабылдау

Сіз KSN бағдарламасын KSN қосу кезінде оқитын және қабылдайтын KSN мәлімдемесіне сай қолданасыз. KSN мәлімдемесі жаңартылған болса, ол басқару серверін алдыңғы нұсқасынан жаңарту кезінде көрсетіледі. Сіз жаңартылған KSN мәлімдемесін қабылдауға немесе қабылдамауға болады. Оны қабылдамасаңыз, сіз бұған дейін қабылдаған KSN мәлімдемесінің нұсқасына сәйкес KSN бағдарламасын қолдануды жалғастырасыз.

Басқару серверін алдыңғы нұсқасынан жаңартқаннан кейін, жаңартылған KSN мәлімдемесі автоматты түрде көрсетіледі. Жаңартылған KSN мәлімдемесін қабылдамасаңыз, оны бәрібір кейінірек қарап шыға аласыз және қабылдай аласыз.

Жаңартылған KSN мәлімдемесін қарап шығу және қабылдау немесе қабылдамау үшін:

1. Бағдарламаның басты терезесінің жоғарғы оң жақ бұрышындағы **Хабарландыруларды қарау** белгішесін басыңыз.

   Хабарландырулар терезесі ашылады.

2. **Жаңартылған KSN мәлімдемесін қарау** сілтемесінен өтіңіз.

   Kaspersky Security Network мәлімдемесін жаңарту терезесі ашылады.

3. KSN мәлімдемесін оқып шығыңыз, содан соң келесі түймелердің бірін басып, шешім қабылдаңыз:

   - **Мен жаңартылған KSN мәлімдемесінің шарттарын қабылдаймын**
   - **Ескі KSN мәлімдемесі бар KSN қолдану**

Сіздің таңдауыңызға байланысты KSN ағымдағы немесе жаңартылған KSN мәлімдемесінің шарттарына сәйкес жұмысын жалғастырады. Сіз кез келген уақытта қабылданған KSN мәлімдемесі мәтінін Басқару сервері сипаттарынан көре аласыз.

Тарату нүктесі KSN прокси-сервері ретінде жұмыс істейтінін тексеру

Тарату нүктесі рөлін атқаратын басқарылатын құрылғыда KSN прокси-серверін қосуға болады. Басқарылатын құрылғыда ksnproxy қызметі іске қосылған болса, ол KSN прокси-сервері ретінде жұмыс істейді. Бұл қызметті құрылғыда жергілікті түрде қосуға немесе өшіруге болады.

Windows немесе Linux операциялық жүйесі бар құрылғыны тарату нүктесі ретінде тағайындауға болады. Тарату нүктесі қалай тексерілетіні осы тарату нүктесінің операциялық жүйесіне байланысты.

Тарату нүктесі Windows операциялық жүйесімен KSN прокси-сервері ретінде жұмыс істейтінін тексеру үшін:

1. Тарату нүктесі рөлін атқаратын құрылғыда Windows операциялық жүйесінде **Қызметтер** терезесін ашыңыз (**Барлық бағдарламалар** → **Басқару** → **Қызметтер**).

2. Қызметтер тізімінде KSN – ksnproxy прокси-сервері қызметі жұмыс істеп тұрғанын тексеріңіз.

   Егер ksnproxy қызметі жұмыс істеп тұрса, онда құрылғыдағы Желілік агент Kaspersky Security Network бағдарламасына қатысады және тарату нүктесінің әрекет ету ауқымына кіретін басқарылатын құрылғылар үшін KSN Proxy прокси-сервері ретінде жұмыс істейді.

Қажет болса, ksnproxy қызметін өшіруге болады. Бұл жағдайда, тарату нүктесінде Желілік агент бұдан былай Kaspersky Security Network бағдарламасына қатыспайды. Бұл үшін, жергілікті әкімші құқықтары керек.

Тарату нүктесі Linux операциялық жүйесімен KSN прокси-сервері ретінде жұмыс істейтінін тексеру үшін:

1. Тарату нүктесі ретінде әрекет ететін құрылғыда іске қосылған процестердің тізімі көрсетіледі.

2. Іске қосылған процестер тізімінде `/opt/kaspersky/ksc64/sbin/ksnproxy` процесінің іске қосылғанын тексеріңіз.

Егер `/opt/kaspersky/ksc64/sbin/ksnproxy` процесі іске қосылып тұрса, онда құрылғыдағы Желілік агент Kaspersky Security Network бағдарламасына қатысады және тарату нүктесінің әрекет ету ауқымына кіретін басқарылатын құрылғылар үшін KSN прокси-сервері ретінде жұмыс істейді.

Сценарий: Kaspersky Security Center және басқарылатын қауіпсіздік бағдарламаларын жаңарту

Бұл бөлімде Kaspersky Security Center бағдарламасы мен басқарылатын қауіпсіздік бағдарламаларын жаңартудың негізгі сценарийі сипатталған.

Kaspersky Security Center және басқарылатын қауіпсіздік бағдарламаларын жаңарту келесі кезеңдерден тұрады:

1. **Жабдыққа және бағдарламалық жасақтамаға қойылатын талаптарды тексеру**

   Жабдықтың талаптарға сай келетініне көз жеткізіңіз және қажетті жаңартуларды орнатыңыз.

2. **Ресурстарды жоспарлау**

   Дерекқор қанша диск кеңістігін алатынын есептеңіз. Қатты дискіде Басқару сервері деректерінің сақтық көшірмесін сақтау үшін жеткілікті бос орын бар екеніне көз жеткізіңіз.

3. **Kaspersky Security Center орнату файлын алу**

   Kaspersky Security Center ағымдағы нұсқасы үшін орындалатын файлды алыңыз және оны Басқару сервері рөлін атқаратын құрылғыға сақтаңыз. Сіз пайдаланып жатқан Kaspersky Security Center нұсқасының шығарылымы туралы ақпаратты қараңыз.

4. **Алдыңғы нұсқаның сақтық көшірмесін жасау**

   Деректерді сақтық көшірмелеу және қалпына келтіру утилитасын пайдаланып, Басқару сервері деректерін сақтық көшірмелеңіз. Сондай-ақ, сақтық көшірмелеу тапсырмасын жасауға болады.

   Орнатылған плагиндердің тізімін экспорттау ұсынылады.

5. **Орнатушыны іске қосу**

   Kaspersky Security Center соңғы нұсқасы үшін орындалатын файлды іске қосыңыз. Файлды іске қосқаннан кейін, оның сақтық көшірмесі жасалғанын және оған апаратын жолды көрсетіңіз. Сақтық көшірмеден деректерді қалпына келтіру жүзеге асырылады.

6. **Басқарылатын бағдарламаларды жаңарту**

   Егер жаңа нұсқасы қолжетімді болса, бағдарламаны жаңартуға болады. Kaspersky қолдау көрсетілетін бағдарламаларының тізімін қарап шығыңыз және Kaspersky Security Center нұсқасының осы бағдарламамен үйлесімді екеніне көз жеткізіңіз. Содан кейін, шығарылым туралы ақпаратта сипатталғандай бағдарламаны жаңартыңыз.

Нәтижелер

Жаңарту сценарийі аяқталғаннан кейін, Басқару серверінің жаңа нұсқасы Басқару консолінде (MMC) сәтті орнатылғанына көз жеткізіңіз. Мәзірден **Анықтама** → **Kaspersky Security Center туралы** тармағын таңдаңыз. Бағдарлама нұсқасының нөмірі көрсетіледі.

Kaspersky Security Center Web Console веб-консолінде Басқару серверінің соңғы нұсқасын пайдаланып жатқаныңызға көз жеткізіңіз, экранның жоғарғы жағында Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз. Ашылған Басқару сервері сипаттары терезесінде, **Жалпы** қойыншасында **Жалпы** бөлімін таңдаңыз. Бағдарлама нұсқасының нөмірі көрсетіледі.

Басқару сервері деректерін қалпына келтіру қажет болса, келесі бөлімде сипатталған қадамдарды орындаңыз: Интерактивті режимде сақтық көшірмелеу және деректерді қалпына келтіру.

Егер сіз басқарылатын қауіпсіздік бағдарламасын жаңартқан болсаңыз, оның басқарылатын құрылғыларда дұрыс орнатылғанына көз жеткізіңіз. Қосымша ақпарат алу үшін осы бағдарламаның құжаттамасын қараңыз.

Kaspersky дерекқорлары мен бағдарламаларын жаңарту

Бұл бөлімде тұрақты жаңартулар үшін орындау керек қадамдар сипатталған:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;
- Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Сценарий: Kaspersky бағдарламалары мен дерекқорларын үнемі жаңартып тұру

Бұл бөлімде Kaspersky дерекқорлары, бағдарламалық модульдері мен бағдарламаларын үнемі жаңартып тұру сценарийі ұсынылған. Сіз Ұйымның желісінде қорғанысты конфигурациялау сценарийін аяқтағаннан кейін, Басқару серверлері мен басқарылатын құрылғыларды түрлі қауіптерден, сонымен қатар вирустардан, желілік шабуылдардан және фишингтік шабуылдардан қорғауды қамтамасыз ету үшін қорғаныс жүйесінің сенімділігін қамтамасыз етуге тиіссіз.

Желі қорғанысына, келесіні үнемі жаңартып тұру арқылы қолдау көрсетіледі:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;
- Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

Сіз осы сценарийді аяқтағаннан кейін, келесіге сенімді бола аласыз:

- Сіздің желіңіз Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky ең соңғы бағдарламалық жасақтамасымен қорғалған.
- Желі қауіпсіздігі үшін критикалық тұрғыдан маңызды болып саналатын Kaspersky антивирустық дерекқорлары мен басқа да дерекқорлары, әрдайым өзекті.

Алдын ала талаптар

Басқарылатын құрылғылардың Басқару серверімен қосылымы болуы тиіс. Құрылғылардың қосылымы болмаса, Kaspersky дерекқорлары, бағдарламалық модульдері мен бағдарламаларын қолмен немесе тікелей Kaspersky жаңарту серверлерінен жаңарту мүмкіндігін қарастырып көріңіз.

Басқару серверінің интернетке қосылымы болуы тиіс.

Бастамас бұрын, келесі әрекеттерді орындағаныңызға көз жеткізіңіз:

1. Kaspersky Security Center Web Console көмегімен Kaspersky бағдарламалық жасақтамасын орналастыру сценарийіне сәйкес басқарылатын құрылғыларда Kaspersky қауіпсіздік бағдарламалары орналастырылды.

2. Желі қорғанысын конфигурациялау сценарийіне сәйкес барлық қажетті саясаттар, саясат профильдері және тапсырмалар жасалған және конфигурацияланған.

3. Басқарылатын құрылғылардың санына және желі топологиясына сәйкес тарату нүктелерінің тиісті саны тағайындалған.

Kaspersky бағдарламалары мен дерекқорларын жаңарту келесі кезеңдерден тұрады:

1. **Жаңарту схемасын таңдау**

   Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларының жаңартуларын орнату үшін қолдануға болатын бірнеше схема бар. Желіңіздің талаптарына бәрінен жақсы сай келетін схеманы немесе бірнеше схеманы таңдап алыңыз.

2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау**

   Бұл тапсырма Kaspersky Security Center бағдарламы жылдам іске қосу шеберінде автоматты түрде жасалады. Бағдарламы жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы дәл қазір жасаңыз.

   Бұл тапсырма жаңартуларды Kaspersky жаңартулар серверлерінен Басқару сервері қоймасына, сондай-ақ Kaspersky Security Center үшін дерекқорлар мен бағдарламалық модульдердің жаңартуларын жүктеп алуға қажет. Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

   Сіздің желіңізде тарату нүктелері тағайындалған болса, жаңартулар Басқару серверінің қоймасынан тарату нүктелерінің қоймаларына автоматты түрде жүктеледі. Бұл жағдайда, тарату нүктесінің ауқымына кіретін басқарылатын құрылғылар Басқару серверінің қоймасы орнына жаңартуларды тарату нүктелерінің қоймаларынан жүктеп алады.

   Нұсқаулар:

   - Басқару консолі: Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау.
   - Kaspersky Security Center Web Console: Жаңартуларды Басқару серверінің қоймасына жүктеп алу үшін тапсырма жасау.

3. **Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау (қажет болса)**

   Әдепкі бойынша, жаңартулар Басқару сервері қоймасынан тарату нүктелерінің қоймаларына жүктеледі. Сіз Kaspersky Security Center бағдарламасын, тарату нүктелері жаңартуларды тікелей Kaspersky жаңарту серверлерінен жүктейтін етіп конфигурациялай аласыз. Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса, жаңартулары тарату нүктелерінің қоймаларынан жүктеп алу артық көрінеді.

Сіздің желіңізге тарату нүктелері тағайындалып, *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы жасалған кезде, тарату нүктелері жаңартуларды Басқару сервері қоймасынан емес, Kaspersky жаңарту серверлерінен жүктейді.

Нұсқаулар:

- Басқару консолі: Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау.
- Kaspersky Security Center Web Console: Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау.

4. **Тарату нүктелерін конфигурациялау**

Сіздің желіңізге тарату нүктелері тағайындалған болса, **Жаңартуларды тарату** параметрі барлық қажетті тарату нүктелеріндегі сипаттарда қосылғанына көз жеткізіңіз. Егер бұл параметр тарату нүктесі үшін өшірулі болса, тарату нүктесінің ауқымына қосылған құрылғылар Басқару сервері қоймасынан жаңартуларды жүктейді.

Егер сіз басқарылатын құрылғылардың тек тарату нүктелерінен жаңартулар алуын қаласаңыз, Желілік агент саясатындағы **Файлдарды тек тарату нүктелері арқылы тарату** параметрін қосыңыз.

5. **Жаңартуларды алудың немесе айырмашылық файлдарын жүктеудің офлайн моделін қолдана отырып, жаңарту процесін оңтайландыру (қажет болса)**

Жаңарту процесін, жаңартуларды жүктеудің офлайн моделін (әдепкі бойынша қосылған) немесе айырмашылық файлдарын пайдалану арқылы оңтайландыруға болады Әрбір желі сегменті үшін осы екі функцияның қайсысын қосу керектігін таңдау керек, өйткені олар бір уақытта жұмыс істей алмайды.

Жаңартуларды алудың офлайн моделі қосылған кезде, қауіпсіздік бағдарламасы жаңартуларды сұрамас бұрын, Желілік агент жаңартуларды Басқару сервері қоймасына жүктегеннен кейін басқарылатын құрылғыға қажетті жаңартуларды жүктейді. Бұл жаңарту процесінің сенімділігін арттырады. Бұл функцияны пайдалану үшін Желілік агент саясаты тапсырмасының сипаттарындағы **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)** параметрін қосыңыз.

Егер сіз жаңартуларды жүктеудің офлайн моделін пайдаланбасаңыз, айырмашылық файлдарын қолдана отырып, Басқару сервері мен басқарылатын құрылғылар арасындағы трафикті оңтайландыруға болады. Бұл функция қосылған кезде, Басқару сервері немесе тарату нүктесі Kaspersky бүкіл дерекқор файлдарының немесе бағдарламалық модульдерінің орнына айырмашылық файлдарын жүктейді. Айырмашылықтар файлы дерекқор немесе бағдарламалық модуль файлдарының екі нұсқасы арасындағы айырмашылықтарды сипаттайды. Сондықтан, айырмашылық файлдары бүкіл файлдарға қарағанда аз орын алады. Нәтижесінде, Басқару сервері немесе тарату нүктелері және басқарылатын құрылғылар арасындағы трафик азаяды. Бұл функцияны пайдалану үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* және/немесе *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының сипаттарындағы **diff файлдарды жүктеп алу** параметрін қосыңыз.

Нұсқаулар:

- Kaspersky дерекқорлары мен бағдарламалық модульдерін жаңарту үшін айырмашылық файлдарын пайдалану.
- Басқару консолі: Жаңартуларды алудың офлайн-моделін қосу және өшіру.
- Kaspersky Security Center Web Console: Басқару консолі: Жаңартуларды алудың офлайн моделін қосу және өшіру.

6. **Алынған жаңартуларды тексеру (қажет болса)**

Жүктелген жаңартуларды орнатпас бұрын, *Жаңартуларды тексеру* тапсырмасын пайдаланып, жаңартуларды тексеруге болады. Бұл тапсырма құрылғыны жаңарту тапсырмаларын және аталған сынақ құрылғыларының жиынтығына арналған параметрлермен конфигурацияланған зиянды БҚ іздеу тапсырмаларын дәйекті түрде іске қосады. Тапсырма нәтижелерін алғаннан кейін, Басқару сервері жаңартуларды қалған құрылғыларға таратуды бастайды немесе бұғаттайды.

Жаңартуларды тексеру тапсырмасы *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының бөлігі ретінде орындалуы мүмкін. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы сипаттарында, Басқару консолінде **Тарату алдында жаңартулар бар-жоғын тексеруді орындау** параметрін немесе Kaspersky Security Center Web Console веб-консолінде **Жаңарту тексерісін іске қосу** параметрін қосыңыз.

Нұсқаулар:

- Басқару консолі: Алынған жаңартуларды тексеру.
- Kaspersky Security Center Web Console: Алынған жаңартуларды тексеру.

7. **Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау**

Әдепкі бойынша, жүктелген бағдарламалық жасақтама жаңартулары *Анықталмаған* күйіне ие. Жаңарту күйін *Расталды* немесе *Қабылданбады* күйіне өзгертуге болады. Бекітілген жаңартулар әрқашан орнатылады. Егер жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдауыңыз қажет. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін. Анықталмаған жаңартуларды тек Желілік агентке және Kaspersky Security Center басқа құрамдастарына Желілік агент саясатының параметрлеріне сәйкес орнатуға болады. Сіз *Қабылданбады* деп белгілеген жаңартулар, басқарылатын құрылғыларға орнатылмайды. Егер қауіпсіздік бағдарламасы үшін бұрын қабылданбаған жаңарту орнатылған болса, Kaspersky Security Center барлық бағдарламасы құрылғылардан жаңартуларды жоюға тырысады.

Жаңартуларды мақұлдау және қабылдамау Windows операциялық жүйесімен жұмыс істейтін клиент құрылғыларына орнатылған желілік агент пен Kaspersky басқарылатын қолданбалары үшін ғана қолжетімді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
- Kaspersky Security Center Web Console: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау.

8. **Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнатуды конфигурациялау**

Желілік агентке және Kaspersky Security Center басқа құрамдастарына жүктелген жаңартулар мен патчтар автоматты түрде орнатылады. Егер сіз Желілік агенттің сипаттарында **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату** параметрін қосулы қалдырсаңыз, онда барлық жаңартулар қоймаға (немесе бірнеше қоймаға) жүктелгеннен кейін автоматты түрде орнатылады. Егер жалауша алынып тасталса, *Анықталмаған* мәртебесі бар Kaspersky жүктелген патчтары, әкімші олардың мәртебесін *Расталды* деп өзгерткеннен кейін орнатылады.

Нұсқаулар:

- Басқару консолі: Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру.
- Kaspersky Security Center Web Console: Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру.

9. **Басқару сервері үшін жаңартуларды орнату**

Басқару серверіне арналған бағдарламалық жасақтама жаңартулары жаңарту күйлеріне тәуелді емес. Олар автоматты түрде орнатылмайды және Басқару консолінде Мониторинг қойыншасында (**Басқару сервері** `<Сервер атауы>` → **Мониторинг**) немесе Kaspersky Security Center Web Console веб-консолінде **Хабарландырулар** бөлімінде (**Бақылау және есеп беру** → **Хабарландырулар**) әкімші тарапынан алдын ала мақұлдануы тиіс. Осыдан кейін, әкімші жаңартуларды орнатуды нақты түрде бастауы керек.

10. **Қауіпсіздік бағдарламалары үшін жаңартуларды автоматты түрде орнатуды конфигурациялау**

    Kaspersky бағдарламаларын, бағдарламалық модульдерін және дерекқорларын, соның ішінде антивирустық базаларды уақтылы жаңартуды қамтамасыз ету мақсатында, басқарылатын бағдарламалар үшін *Жаңарту* тапсырмасын жасаңыз. Уақтылы жаңарту үшін тапсырмалар кестесін конфигурациялау кезінде **Қоймаға жаңартуларды жүктеу кезінде** параметрін таңдау ұсынылады.

    Егер сіздің желіңізде тек IPv6 қолдайтын құрылғылар болса және сіз осы құрылғыларда орнатылған қауіпсіздік бағдарламаларын үнемі жаңартып отырғыңыз келсе, басқарылатын құрылғыларда Басқару сервері (13.2 немесе одан жоғары нұсқалар) және Желілік агент (13.2 немесе одан жоғары нұсқалар) орнатылғанына көз жеткізіңіз.

    Әдепкі бойынша, Kaspersky Endpoint Security for Windows және Kaspersky Endpoint Security for Linux үшін жаңартулар тек жаңарту күйі *Расталды* болып өзгертілгеннен кейін ғана орнатылады. *Жаңарту* тапсырмасында жаңарту параметрлерін өзгертуге болады.

    Егер жаңарту Лицензиялық келісімнің шарттарын қабылдауды талап етсе, алдымен Лицензиялық келісімнің шарттарын оқып, қабылдауыңыз қажет. Осыдан кейін, жаңартулар басқарылатын құрылғыларға таратылуы мүмкін.

    Нұсқаулар:

    - Басқару консолі: Құрылғыларға Kaspersky Endpoint Security жаңартуларын автоматты түрде орнату.
    - Kaspersky Security Center Web Console: Басқару консолі: Құрылғыларға Kaspersky Endpoint Security жаңартуларын автоматты түрде орнату.

Нәтижелер

Сценарий аяқталғаннан кейін, Kaspersky Security Center бағдарламасы Басқару сервері қоймасына немесе тарату нүктелерінің қоймаларына жаңартуларды жүктегеннен кейін, Kaspersky дерекқорларын және Kaspersky орнатылған бағдарламаларын жаңартуға арналған. Енді сіз желі жұмысын бақылауға кірісе аласыз.

Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту туралы

Басқару серверлері мен басқарылатын құрылғыларды қорғау жаңартылған күйде екеніне көз жеткізу үшін келесі жаңартуларды уақтылы ұсыну керек:

- Kaspersky дерекқорлары мен бағдарламалық модульдері;

  Kaspersky Security Center бағдарламасы Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктемес бұрын Kaspersky серверлерінің қолжетімділігін тексереді. Жүйелік DNS арқылы серверлерге қатынасу мүмкін болмаса, бағдарлама жалпыға ортақ DNS серверлерін пайдаланады. Бұл антивирустық дерекқорларды жаңарту және басқарылатын құрылғылардың қауіпсіздік деңгейін сақтау үшін қажет.

- Kaspersky Security Center құрамдастары мен қауіпсіздік бағдарламаларын қоса алғанда, Kaspersky орнатылған бағдарламалары.

  Kaspersky Security Center сізге Windows жүйесімен жұмыс істейтін клиенттік құрылғыларда орнатылған Желілік агент пен Kaspersky қолданбаларын автоматты түрде жаңартуға мүмкіндік береді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді. Бұл компоненттерді жаңарту үшін, олардың соңғы нұсқаларын Kaspersky сайтынан жүктеп алу және қолмен орнату керек.

Желіңіздің конфигурациясына байланысты сіз келесі жүктеу схемаларын қолдана аласыз және басқарылатын құрылғыларға қажетті жаңартуларды тарата аласыз:

- Бір тапсырмамен: *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*
- Екі тапсырманың көмегімен:
  - *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмалары.
  - *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмалары.
- Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен
- Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін Kaspersky жаңарту серверлерінен тікелей
- Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын пайдалану

Бұл схемада Kaspersky Security Center жаңартуларды *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы арқылы жүктейді. Желінің бір сегментінде 300-ден аз басқарылатын құрылғы немесе әр сегментте оннан аз басқарылатын құрылғы бар шағын желілерде, жаңартулар басқарылатын құрылғыларға тікелей Басқару серверінің қоймасынан таралады (төмендегі суретті қараңыз).

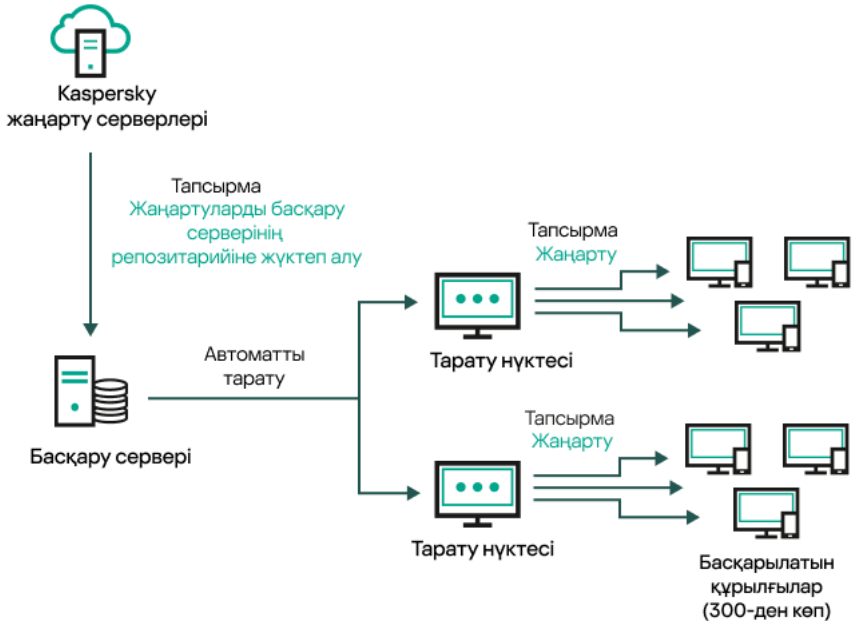


Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолдану арқылы және тарату нүктелерінсіз жаңарту

Әдепкі бойынша, Басқару сервері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Егер сіздің желіңізде бір желі сегментінде 300-ден астам басқарылатын құрылғы болса немесе сіздің желіңізде тоғыздан астам басқарылатын құрылғысы бар бірнеше сегмент болса, жаңартуларды басқарылатын құрылғыларға тарату үшін тарату нүктелерін пайдалануды ұсынамыз (төмендегі суретті қараңыз). Тарату нүктелері Басқару серверіне түсетін жүктемені азайтады және Басқару сервері мен басқарылатын құрылғылар арасындағы трафикті оңтайландырады. Тарату нүктелерінің санын және олардың желіңізге қажетті конфигурациясын есептеуіңізге болады.

Бұл схемада жаңартулар Басқару сервері қоймасынан тарату нүктесінің қоймаларына автоматты түрде жүктеледі. Тарату нүктесінің ауқымына кіретін басқарылатын құрылғылар Басқару серверінің қоймасы орнына жаңартуларды тарату нүктелерінің қоймаларынан жүктеп алады.



Тарату нүктелері бар Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолдану арқылы жаңарту

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы аяқталғаннан кейін, келесі жаңартулар Басқару серверінің қоймасына жүктеледі:

- Kaspersky Security Center үшін Kaspersky дерекқорлары мен бағдарламалық модульдері.

  Бұл жаңартулар автоматты түрде орнатылады.

- Басқарылатын құрылғылардағы қауіпсіздік бағдарламаларына арналған Kaspersky дерекқорлары мен бағдарламалық модульдері.

  Бұл жаңартулар Kaspersky Endpoint Security for Windows жаңарту тапсырмасы арқылы орнатылады.

- Басқару серверіне арналған жаңартулар.

  Бұл жаңартулар автоматты түрде орнатылмайды. Әкімші жаңартуларды нақты мақұлдап, жаңартуларды орнатуды іске қосуы керек.

  > Басқару серверіне патчтарды орнату үшін жергілікті әкімші құқықтары қажет.

- Kaspersky Security Center құрамдастарына арналған жаңартулар.

  Әдепкі бойынша, бұл жаңартулар автоматты түрде орнатылады. Сіз Желілік агент саясатының параметрлерін өзгерте аласыз.

- Қауіпсіздік бағдарламаларына арналған жаңартулар.

  Әдепкі бойынша, Kaspersky Endpoint Security for Windows бағдарламасы сіз мақұлдаған жаңартуларды ғана орнатады. (Сіз Басқару консолі немесе Kaspersky Security Center Web Console арқылы жаңартуларды мақұлдай аласыз). Жаңартулар *Жаңарту* тапсырмасы арқылы орнатылады және сол тапсырманың сипаттарында конфигурациялануы мүмкін.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы жүктеп алу тапсырмасы виртуалды Басқару серверлерінде қолжетімді емес. Виртуалды сервердің қоймасы негізгі Басқару серверіне жүктелген жаңартуларды көрсетеді.

Алынған жаңартуларды жұмысқа жарамдылық тұрғысынан және сынақ құрылғыларының жиынтығында қателердің болуы тұрғысынан тексеруге конфигурациялауға болады. Егер тексеру сәтті болса, жаңартулар басқа басқарылатын құрылғыларға таралады.

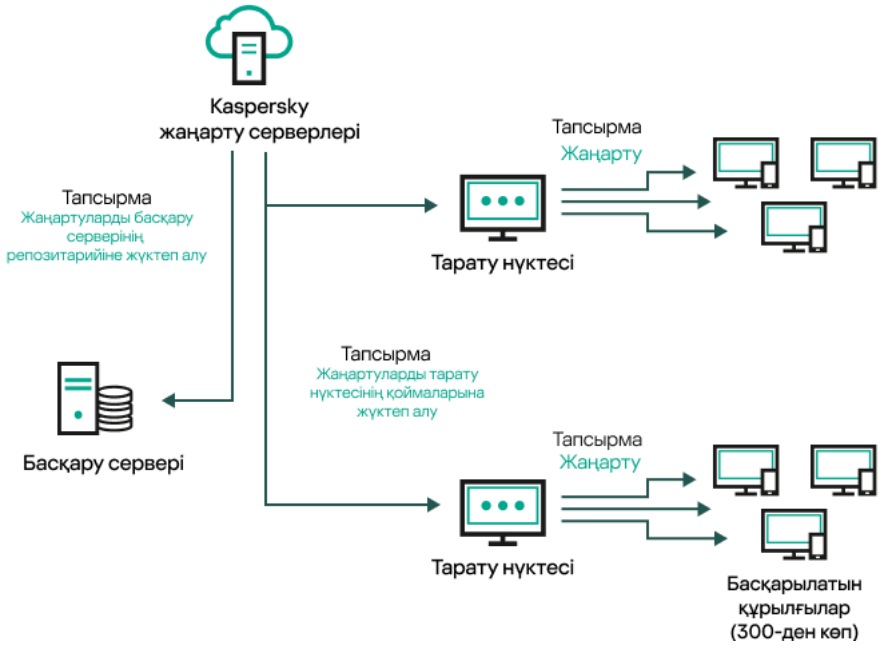
Әрбір басқарылатын Kaspersky бағдарламасы Басқару серверінен қажетті жаңартуларды сұрайды. Басқару сервері осы сұрауларды біріктіреді және тек бағдарламалар сұрайтын жаңартуларды жүктейді. Осылайша, тек қажетті жаңартулар және тек бір рет қана жүктелетіні қамтамасыз етіледі. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын орындау кезінде Kaspersky дерекқорлары мен бағдарламалық модульдерінің қажетті нұсқаларының жүктелуін қамтамасыз ету үшін Kaspersky жаңарту серверлеріне автоматты түрде Басқару сервері мынадай ақпаратты жібереді:

- Бағдарламаның идентификаторы және нұсқасы
- Қолданбаны орнату идентификаторы
- Белсенді кілт идентификаторы
- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын іске қосу идентификаторы

Берілетін ақпарат дербес деректерді және басқа да құпия деректерді қамтымайды. АО "Лаборатория Касперского" алынған ақпаратты заңда белгіленген талаптарға сәйкес қорғайды.

Екі тапсырманы пайдалану: Жаңартуларды Басқару серверінің қоймасына жүктеп алу және Жаңартуларды тарату орындарының қоймаларына жүктеп алу

Тарату нүктелерінің қоймаларына жаңартуларды Басқару сервері қоймасының орнына тікелей Kaspersky жаңарту серверлерінен жүктеп алуға болады, содан кейін жаңартуларды басқарылатын құрылғыларға таратуға болады (төмендегі суретті қараңыз). Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса, жаңартулары тарату нүктелерінің қоймаларынан жүктеп алу артық көрінеді.



Жаңартуларды Басқару серверінің қоймасына жүктеп алу және Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмалары көмегімен жаңарту

Әдепкі бойынша, Басқару сервері мен тарату нүктелері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін және/немесе тарату нүктелерін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

Бұл схеманы іске асыру үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасына қосымша ретінде *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын жасаңыз. Осыдан кейін, тарату нүктелері жаңартуларды Басқару серверінің қоймасынан емес, Kaspersky жаңарту серверлерінен жүктейді.

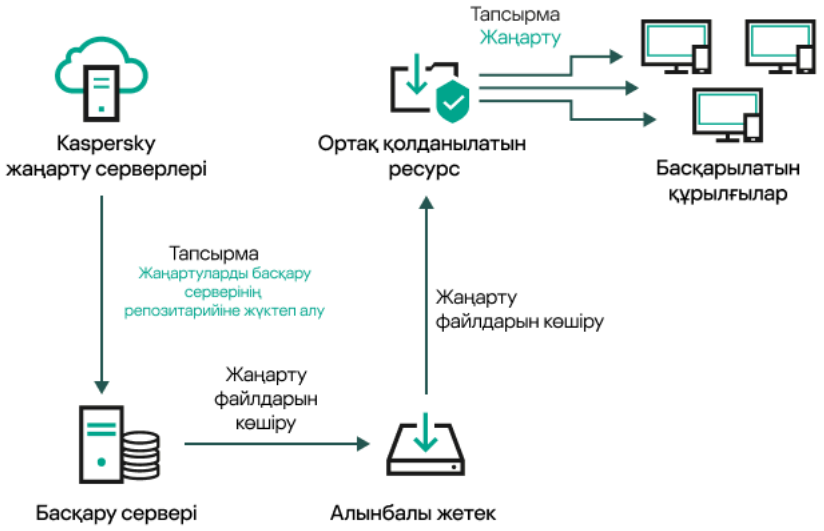
macOS басқаруындағы тарату нүктелері Kaspersky жаңарту серверлерінен жаңартуларды жүктеп ала алмайды.

macOS операциялық жүйесі бар құрылғылар *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасының әрекет ету ауқымында болса, онда тапсырма Windows операциялық жүйесі бар құрылғылардың барлығында сәтті аяқталса да, *Сәтсіз аяқталды* мәртебесімен аяқталады.

Бұл схема үшін де *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы керек, себебі бұл тапсырма Kaspersky Security Center үшін Kaspersky дерекқорлары мен бағдарламалық модульдерін жүктеу үшін қолданылады.

Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы қолмен

Егер клиент құрылғылары Басқару серверіне қосылмаған болса, сіз жергілікті қалтаны немесе ортақ ресурсты Kaspersky дерекқорларын, бағдарламалық модульдерін және бағдарламаларын жаңарту көзі ретінде пайдалана аласыз. Бұл схемада қажетті жаңартуларды Басқару сервері қоймасынан алынбалы дискіге көшіру керек, содан кейін жаңартуларды жергілікті қалтаға немесе Kaspersky Endpoint Security параметрлерінде жаңарту көзі ретінде көрсетілген ортақ ресурсқа көшіру керек (төмендегі суретті қараңыз).



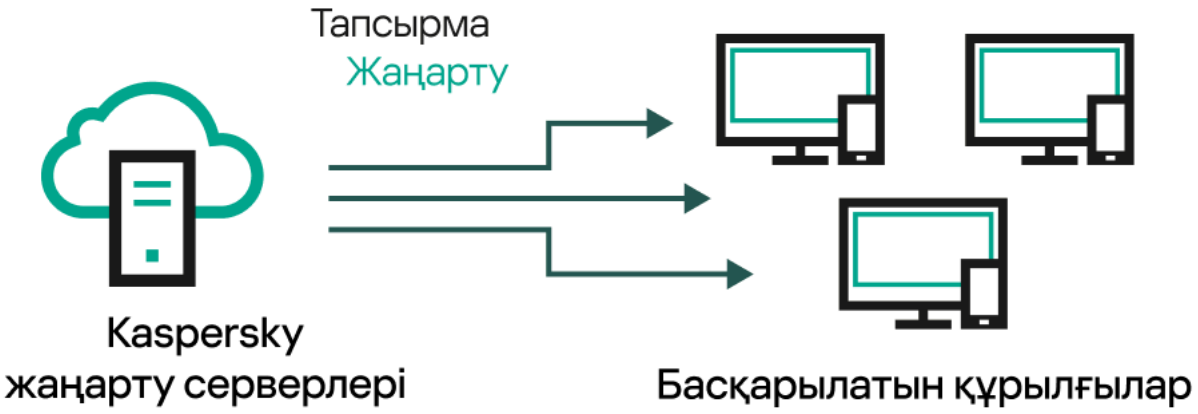
Жергілікті қалта, ортақ қатынасы бар қалта немесе FTP сервері арқылы жаңарту

Kaspersky Endpoint Security бағдарламасындағы жаңарту көздері туралы қосымша ақпарат алу үшін келесі анықтамаларды қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы

Басқарылатын құрылғылардағы Kaspersky Endpoint Security үшін Kaspersky жаңарту серверлерінен тікелей

Басқарылатын құрылғыларда сіз Kaspersky Endpoint Security бағдарламасын Kaspersky жаңарту серверлерінен тікелей жаңартуларды алу үшін конфигурациялай аласыз (төмендегі суретті қараңыз).



Қауіпсіздік бағдарламаларын тікелей Kaspersky жаңарту серверлерінен жаңарту

Бұл схемада қауіпсіздік бағдарламалары Kaspersky Security Center ұсынған қоймаларды пайдаланбайды. Жаңартуларды тікелей Kaspersky жаңарту серверлерінен алу үшін қауіпсіздік бағдарламасының интерфейсіндегі жаңарту көзі ретінде Kaspersky жаңарту серверлерін көрсетіңіз. Осы параметрлер туралы қосымша ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы

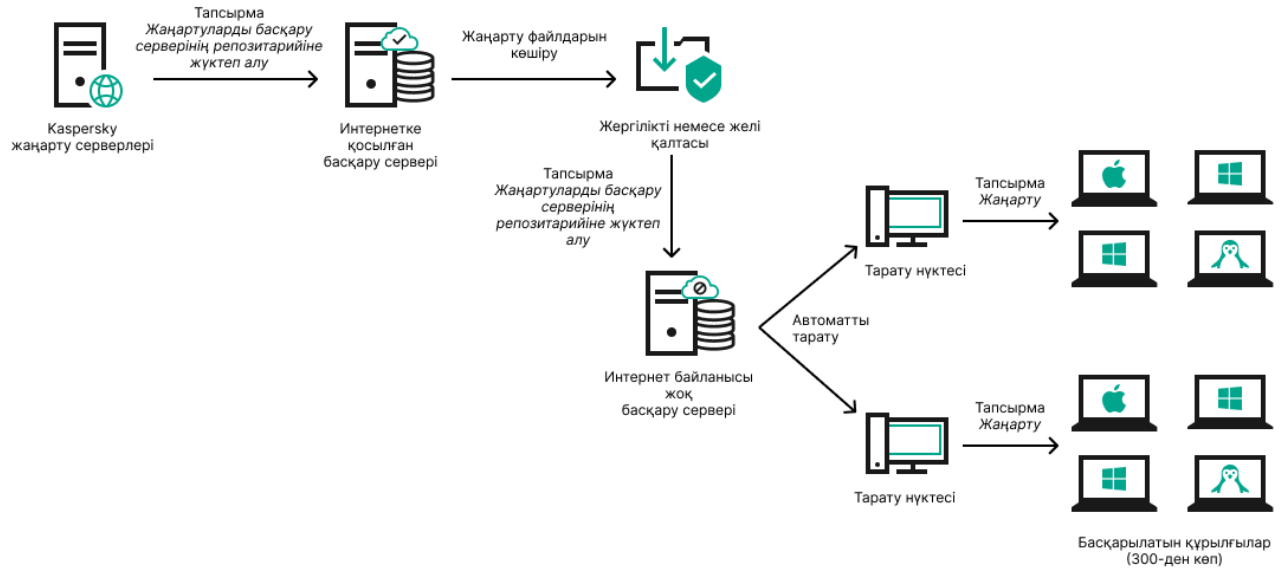
Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы

Басқару серверінде интернет қосылымы болмаса, жергілікті немесе желілік қалтадан жаңартуларды жүктеу үшін *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын конфигурациялауға болады. Бұл жағдайда, қажетті жаңарту файлдарын көрсетілген қалтаға мезгіл-мезгіл көшіріп тұру қажет. Мысалы, қажетті жаңарту файлдарын келесі көздердің бірінен көшіруге болады:

- Интернетке кіру мүмкіндігі бар Басқару сервері (төмендегі суретті қараңыз).

  Басқару сервері тек қауіпсіздік бағдарламалары сұрайтын жаңартуларды жүктейтіндіктен, Басқару серверлері басқаратын қауіпсіздік бағдарламаларының жиынтығы (интернетке қосылған және қосылмаған) сәйкес келуі керек.

  Сіз жаңартуларды жүктеу үшін қолданатын Басқару серверінің нұсқасы 13.2 немесе одан да бұрынғы болса, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарын ашып, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.



Басқару сервері интернетке қатынаса алмаса, жергілікті немесе желілік қалта арқылы жаңарту

- Kaspersky Update Utility

  Утилита жаңартуларды жүктеу үшін ескі схеманы қолданатындықтан, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарын ашып, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын жасау

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы Kaspersky Security Center бағдарламаны жылдам іске қосу шебері жұмыс істеп тұрған кезде автоматты түрде жасалады. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы бір данада жасалуы мүмкін. Сондықтан, сіз *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын Басқару серверінің тапсырмалар тізімінен жойылған жағдайда ғана жасай аласыз.

Бұл тапсырма Kaspersky жаңарту серверлерінен Басқару сервері қоймасына жаңартуларды жүктеу үшін қажет. Жаңартулардың тізіміне мыналар кіреді:

- Басқару серверіне арналған дерекқорлар мен бағдарламалық модульдер жаңартулары;
- Kaspersky қауіпсіздік бағдарламаларына арналған дерекқорлар мен бағдарламалық модульдер жаңартулары;
- Kaspersky Security Center құрамдастарын жаңарту;
- Kaspersky қауіпсіздік бағдарламалары жаңартулары.

Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

Жаңартуларды басқарылатын құрылғыларға таратпас бұрын, сіз *Жаңартуларды тексеру* тапсырмасын орындай аласыз. Соның арқасында, Басқару сервері жүктелген жаңартуларды дұрыс орнататындығына және қауіпсіздік деңгейі жаңартулардан төмендемейтіндігіне көз жеткізе аласыз. Таратудың алдында жаңартуларды тексеру үшін, *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттарында **Жаңарту тексерісін іске қосу** параметрін конфигурациялаңыз.

***Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасын жасау үшін:*

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Security Center бағдарламасы үшін **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырма түрін таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
6. **Жасау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

7. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

8. Тапсырма сипаттары терезесінде **Бағдарлама параметрлері** қойыншасында келесі параметрлерді көрсетіңіз:

   - **Жаңартулардың көздері**

     Басқару сервері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:

     - Kaspersky жаңартулар серверлері

       Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері. Әдепкі бойынша, Басқару сервері Kaspersky жаңарту серверлерімен өзара әрекеттеседі және HTTPS жаңартуларын жүктейді. Басқару серверін HTTPS орнына HTTP протоколын пайдалану үшін конфигурациялауға болады.

       Әдепкі бойынша таңдалған.

     - Негізгі Басқару сервері

       Бұл ресурс қосалқы немесе виртуалды Басқару сервері үшін жасалған тапсырмаларға қатысты қолданылады.

     - Жергілікті немесе желілік қалта

       Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін. Желілік қалта түпнұсқалықты тексеруді қажет етсе, тек SMB протоколына қолдау көрсетіледі. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

       > Жаңарту көзі ретінде пайдаланылатын FTP серверінде, HTTP серверінде немесе желілік қалтада Kaspersky жаңарту серверлерін пайдалану кезінде жасалған қалталар құрылымына сәйкес келетін қалталар құрылымы (жаңартулармен бірге) болуы керек.

     Егер жаңартулары бар ортақ қатынасы бар қалтасы құпиясөзбен қорғалған болса, **Жаңарту көзінің ортақ қалтасына қатынасу үшін есептік жазбаны көрсетіңіз (болған жағдайда)** параметрін қосып, қатынасу үшін қажетті есептік деректерді енгізіңіз.

   - **Жаңартулар сақталатын қалта**

     Сақталған жаңартуларды сақтау үшін көрсетілген қалтаға апаратын жол. Көрсетілген қалтаға апаратын жолды алмасу буферіне көшіруге болады. Топтық тапсырма үшін көрсетілген қалтаға апаратын жолды өзгерте алмайсыз.

   - Басқа параметрлер:

     - **Қосалқы Басқару серверлерін мәжбүрлеп жаңарту**

       Параметр қосылса, Басқару сервері жаңартуларды алғаннан кейін бірден бағыныңқы Басқару серверлерінде жаңартуларды алу тапсырмаларын іске қосады. Жаңарту тапсырмалары Басқару серверлеріндегі тапсырма сипаттамаларында конфигурацияланған жаңарту көзі арқылы іске қосылады.

       Егер бұл параметр өшірулі болса, қосалқы Басқару серверлеріндегі жаңарту тапсырмалары кестеге сәйкес басталады.

       Әдепкі бойынша, параметр өшірулі.

- **Алынған жаңартуларды қосымша қалталарға көшіру**

  Егер жалауша қойылса, жаңартуларды алғаннан кейін, Басқару сервері жаңартуларды көрсетілген қалталарға көшіреді. Құрылғыңыздағы жаңартуларды қолмен басқарғыңыз келсе, осы параметрді пайдаланыңыз.

  Мысалы, сіз бұл параметрді келесі жағдайда пайдалана аласыз: ұйым желісінде бірнеше тәуелсіз ішкі желілер бар және әр ішкі желідегі құрылғылар басқа ішкі желіге қатынаса алмайды. Бұл жағдайда, барлық ішкі желілердегі құрылғылар ортақ желілік қалтаға қатынаса алады. Бұл жағдайда, ішкі желілердің біріндегі Басқару сервері үшін Kaspersky жаңарту серверлерінен жаңартуларды жүктеуді көрсетіңіз, осы параметрді қосыңыз және осы желілік қалтаны көрсетіңіз. Басқару сервері үшін жаңартуларды қоймаға жүктеу тапсырмасында дәл осы желілік қалтаны жаңартулар көзі ретінде көрсетіңіз.

  Жүктелген жаңартуларды жергілікті қалтаға көшіруді таңдасаңыз, құрылғыда Басқару сервері орнатылған қалтаны көрсетуіңіз керек. Қалтаға апаратын жол құрылғының амалдық жүйесіне байланысты. Жергілікті қалта Linux негізіндегі Басқару серверінде орналасқандықтан, POSIX жолын көрсету керек, мысалы: /path/to/dir.

  Linux негізіндегі Басқару серверінде орналасқан желілік қалтаны таңдағанда, қалтаны іске қосу арқылы Басқару сервері орнатылған құрылғыдан желілік қалтаға қатынасуды алдын ала қамтамасыз ету керек. Қалтаға қатынасу SMB протоколы арқылы жүзеге асырылады.

  Әдепкі бойынша, параметр өшірулі.

- **Көшіру аяқталғанша құрылғыларды және қосалқы Басқару серверлерін мәжбүрлеп жаңартпау**

  Егер жалауша қойылса, клиент құрылғылары және қосалқы Басқару серверлері тарапынан жаңартуларды алу тапсырмалары, жаңартуларды желілік жаңартулар қалтасынан қосымша жаңартулар қалталарына көшіру аяқталғаннан кейін іске қосылады.

  Егер клиент құрылғылары мен қосалқы Басқару серверлері жаңартуларды қосымша желілік қалталардан жүктесе, бұл жалауша қойылуы керек.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартулар мазмұны**:

  - **diff файлдарды жүктеп алу**

    Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

    Әдепкі бойынша, параметр өшірулі.

- **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу**

  14-ші нұсқадан бастап, Kaspersky Security Center бағдарламасы дерекқорлар мен бағдарлама модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Бағдарлама жаңартуларды жаңа схеманың көмегімен жүктей алуы үшін, жаңарту көзі жаңа схемамен үйлесімді метадеректері бар жаңарту файлдарын қамтуы керек. Жаңарту көзінде тек ескі схемамен үйлесімді метадеректері бар жаңарту файлдары болса, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз. Әйтпесе, жаңартуларды жүктеу тапсырмасы қатемен аяқталады.

  Мысалы, жаңарту көзі ретінде жергілікті немесе желілік қалта көрсетілсе және осы қалтадағы жаңарту файлдары келесі бағдарламалардың бірімен жүктелген болса, осы параметрді қосу керек:

  - Kaspersky Update Utility

    Бұл утилита жаңартуларды ескі схема бойынша жүктейді.

- Kaspersky Security Center 13.2 немесе одан бұрынғы нұсқасы

  Мысалы, бір Басқару серверінің интернетке қосылымы жоқ. Бұл жағдайда, сіз интернетке қосылған екінші Басқару сервері арқылы жаңартуларды жүктей аласыз, содан кейін жаңартуларды бірінші Сервер үшін жаңарту көзі ретінде пайдалану үшін жергілікті немесе желілік қалтаға орналастыра аласыз. Егер екінші Басқару серверінде 13.2 немесе одан төмен нұсқа нөмірі болса, бірінші Басқару серверіне арналған тапсырмада **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

Әдепкі бойынша, параметр өшірулі.

- **Жаңарту тексерісін іске қосу**

  Егер жалауша қойылса, Басқару сервері жаңартуларды көзден көшіреді, оларды уақытша қоймада сақтайды және **Жаңартуларды тексеру тапсырмасы** өрісінде көрсетілген Жаңартуларды тексеру тапсырмасын іске қосады. Бұл тапсырма сәтті орындалған жағдайда, жаңартулар уақытша қоймадан Басқару серверінің ортақ қатынас бар қалтасына көшіріледі және Басқару сервері жаңартулардың көзі болып табылатын құрылғыларға таратылады (**Қоймаға жаңартуларды жүктеу кезінде** кесте түрі бар тапсырмалар іске қосылады). Жаңартуларды қоймаға жүктеу тапсырмасы, тек *Жаңартуларды тексеру* тапсырмасы аяқталғаннан кейін аяқталған болып саналады.

  Әдепкі бойынша, параметр өшірулі.

9. Тапсырма сипаттары терезесінде, **Кесте** қойыншасында тапсырманы іске қосу кестесін жасаңыз. Қажет болса, келесі параметрлерді конфигурациялаңыз:

- **Тапсырманы бастау:**

  Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

  - **Қолмен**

    Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **N минут сайын**

    Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

  - **N сағат сайын**

    Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

  - **N күн сайын**

    Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

  - **Апта күндері бойынша**

    Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Ай сайын, таңдалған апталардың көрсетілген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуыл анықталған кезде**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

- Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
- Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

  Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
- Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- **Тапсырма мынанша уақыттан көбірек орындалып жатса, оны тоқтату**

  Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

  Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.

10. **Сақтау** түймесін басыңыз.

    Тапсырма жасалды және конфигурацияланды.

Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен бағдарламалық модульдердің жаңартулары жаңарту көзінен көшіріледі және Басқару серверінің ортақ қатынасы бар қалтасына орналастырылады. Егер тапсырма басқару тобы үшін жасалса, онда ол тек көрсетілген басқару тобына кіретін Желілік агенттерге қолданылады.

Ортақ қатынасы бар қалтадан жаңартулар клиент құрылғыларына және қосалқы Басқару серверлеріне таратылады.

Алынған жаңартуларды тексеру

Басқарылатын құрылғыларға жаңартуларды орнатудың алдында, оларды алдымен *Жаңартуды тексеру* тапсырмасының көмегімен жұмысқа жарамдылығы мен қателері тұрғысынан тексере аласыз. *Жаңартуды тексеру* тапсырмасы *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы аясында автоматты түрде орындалады. Басқару сервері жаңартуларды көзден жүктейді, оларды уақытша қоймада сақтайды және *Жаңартуды тексеру* тапсырмасын іске қосады. Бұл тапсырма сәтті орындалған жағдайда, жаңартулар уақытша қоймадан Басқару серверінің ортақ қатынасы бар қалтасына көшіріледі. Жаңартулар Басқару сервері жаңарту көзі болып табылатын клиент құрылғыларына қолданылады.

Жаңартуды тексеру тапсырмасын орындау нәтижесінде уақытша қоймадағы жаңартулар қате деп танылса немесе *Жаңартуды тексеру* тапсырмасы қатемен аяқталса, мұндай жаңартулар ортақ қалтаға көшірілмейді. Басқару серверінде алдыңғы жаңартулар жиынтығы қалады. **Қоймаға жаңартуларды жүктеу кезінде** кесте түрі бар тапсырмаларды іске қосу да орындалмайды. Жаңа жаңартулар жиынтығын тексеру сәтті аяқталса, бұл операциялар *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасы келесі рет іске қосылған кезде орындалады.

Егер сынақ құрылғыларының кем дегенде біреуінде келесі шарттардың бірі орындалса, жаңартулар жиынтығы дұрыс емес болып саналады:

- жаңарту тапсырмасын орындау кезінде қате пайда болды;
- жаңартуларды қолданғаннан кейін, қауіпсіздік бағдарламасының тұрақты қорғаныс күйі өзгерді;
- талап бойынша тексеру тапсырмасын орындау барысында жұқтырған нысан табылды;
- Kaspersky бағдарламасының жұмыс қатесі туындады.

Егер сынақ құрылғыларының ешқайсысында аталған шарттардың ешбірі орындалмаса, жаңартулар жиынтығы дұрыс деп танылады және *Жаңартуларды тексеру* тапсырмасы сәтті орындалды деп саналады.

Жаңартуды тексеру тапсырмасын жасауға кіріспес бұрын, алдын ала шарттарды орындаңыз:

1. Бірнеше сынақ құрылғысы бар басқару тобын құрыңыз. Жаңартуларды тексеру үшін сізге бұл топ қажет болады.

   Сынақ құрылғылары ретінде ұйымның желісінде ең көп таралған бағдарламалық конфигурациясы бар жақсы қорғалған құрылғыларды пайдалану ұсынылады. Бұл тәсілдеме, тексеру кезінде вирустарды анықтаудың сапасы мен ықтималдығын арттырады, сонымен қатар жалған іске қосылу қаупін азайтады. Сынақ құрылғыларында вирустар табылған кезде *Жаңартуды тексеру* тапсырмасы сәтсіз аяқталды деп саналады.

2. Kaspersky Security Center қолдайтын қолданба үшін (мысалы, Windows-қа арналған Kaspersky Endpoint Security немесе Windows Server-ге арналған Kaspersky Security) жаңарту және зиянды БҚ іздеу тапсырмаларын жасаңыз. Жаңарту және зиянды БҚ іздеу тапсырмаларын жасаған кезде, сынақ құрылғылары бар әкімшілік топты көрсетіңіз.

   Жаңартуды тексеру тапсырмасы барлық жаңартулардың жаңартылғанына көз жеткізу үшін сынақ құрылғыларында жаңарту және зиянды БҚ іздеу тапсырмаларын дәйекті түрде іске қосады. Сондай-ақ, *Жаңартуды тексеру* тапсырмасын жасау кезінде жаңарту және зиянды БҚ іздеу тапсырмаларын көрсету қажет.

3. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын жасаңыз.

Kaspersky Security Center бағдарламасы клиент құрылғыларына таратпас бұрын алынған жаңартуларды тексеруі үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Жаңартуларды Басқару серверінің қоймасына жүктеп алу** тапсырмасының атын басыңыз.

3. Ашылған тапсырма сипаттары терезесінде **Бағдарлама параметрлері** қойыншасына өтіп, **Жаңарту тексерісін іске қосу** параметрін қосыңыз.

4. *Жаңартуларды тексеру* тапсырмасы бар болса, **Тапсырманы таңдау** түймесін басыңыз. Сынақ құрылғылары бар басқару тобында ашылған *Жаңартуларды тексеру* тапсырмасы терезесінде.

5. *Жаңартуларды тексеру* тапсырмасын бұған дейін жасамаған болсаңыз, келесі әрекеттерді орындаңыз:

   a. **Жаңа тапсырма** түймесін басыңыз.

   b. Ашылған тапсырма жасау шеберінде алдын ала орнатылған атауды өзгерткіңіз келсе, тапсырманың атын көрсетіңіз.

   c. Бұрын жасалған сынақ құрылғылары бар басқару тобын таңдаңыз.

   d. Kaspersky Security Center қолдайтын қажетті бағдарламаны жаңарту тапсырмасын таңдаңыз, содан кейін зиянды БҚ іздеу тапсырмасын таңдаңыз.

      Осыдан кейін, келесі параметрлер пайда болады. Оларды қосулы күйде қалдыру ұсынылады:

      - **Дерекқорларды жаңартудан кейін құрылғыны өшіріп қайта қосу**

        Құрылғыдағы антивирустық дерекқорларды жаңартқаннан кейін, құрылғыны қайта іске қосу ұсынылады.

        Әдепкі бойынша, параметр қосулы.

      - **Дерекқорды жаңартып, құрылғыны өшіріп қайта қосқаннан кейін нақты уақыт режимінде қорғау күйін тексеру**

        Егер бұл параметр қосулы болса, *Жаңартуларды тексеру* тапсырмасы Басқару сервері қоймасына жүктелген жаңартулардың өзектілігін және антивирустық дерекқорды жаңартып, құрылғыны қайта іске қосқаннан кейін қорғаныс деңгейінің төмендегенін тексереді.

        Әдепкі бойынша, параметр қосулы.

   e. *Жаңартуларды тексеру* тапсырмасы іске қосылатын есептік жазбаны көрсетіңіз. Сіз өзіңіздің есептік жазбаңызды қолданып, **Әдепкі есептік жазба** параметрін қосулы күйде қалдыра аласыз. Сонымен қатар, тапсырма қажетті қатынасу құқықтары бар басқа есептік жазбада орындалуы керек екенін көрсетуге болады. Ол үшін **Есептік жазбаны көрсету** параметрін таңдап, сол есептік жазбаның есептік деректерін енгізіңіз.

6. *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасының сипаттар терезесін жабу үшін **Сақтау** түймесін басыңыз.

Жаңартуларды автоматты түрде тексеру қосылған. Енді сіз *Жаңартуларды Басқару серверінің қоймасына жүктеп алу* тапсырмасын іске қоса аласыз, сонда ол жаңартуларды тексеруден басталады.

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын жасау

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасы тек Windows басқаруындағы тарату нүктелерімен жұмыс істейді. Linux немесе macOS басқаруындағы тарату нүктесі құрылғылары Kaspersky жаңарту серверлерінен жаңартуларды жүктеп ала алмайды. Linux немесе macOS жүйесімен жұмыс істейтін кем дегенде бір құрылғы тапсырма ауқымында болса, тапсырма *Сәтсіз* күйінде болады. Тіпті тапсырма Windows операциялық жүйесі бар барлық құрылғыларда сәтті аяқталса да, ол басқа құрылғылардағы қатені қайтарады.

Басқару тобы үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын жасай аласыз. Мұндай тапсырма, көрсетілген басқару тобына кіретін тарату нүктелері үшін орындалады.

Бұл тапсырманы, мысалы, Басқару сервері мен тарату нүктелері арасындағы трафик Kaspersky жаңарту серверлері мен тарату нүктелері арасындағы трафиктен қымбатырақ болса немесе Басқару серверіңізде интернетке қатынасу мүмкіндігі болмаса пайдалана аласыз.

Бұл тапсырма Kaspersky жаңарту серверлерінен тарату нүктелері қоймалары жаңартуларды жүктеу үшін қажет. Жаңартулардың тізіміне мыналар кіреді:

- Kaspersky қауіпсіздік бағдарламаларына арналған дерекқорлар мен бағдарламалық модульдер жаңартулары;
- Kaspersky Security Center құрамдастарын жаңарту;
- Kaspersky қауіпсіздік бағдарламалары жаңартулары.

Жаңартуларды жүктегеннен кейін, оларды басқарылатын құрылғыларға таратуға болады.

Егер тарату нүктелері интернетке прокси-сервер арқылы қосылса, Желілік агент саясатында сәйкес параметрлерді көрсету керек.

*Таңдалған басқару тобына **Жаңартуларды тарату орындарының қоймаларына жүктеп алу** тапсырмасын жасау үшін:*

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Security Center бағдарламасы үшін **Task type** өрісінен **Жаңартуларды тарату орындарының қоймаларына жүктеп алу** тармағын таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. Басқару тобын, тапсырма қолданылатын құрылғылар немесе құрылғы таңдауын көрсету үшін таңдау түймесін басыңыз.
6. **Тапсырманы жасауды аяқтау** қадамында, әдепкі бойынша тапсырма параметрлерін өзгерткіңіз келсе, **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосыңыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.
7. **Жасау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.
8. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.
9. Тапсырма сипаттары терезесінің **Бағдарлама параметрлері** қойыншасында келесі параметрлерді көрсетіңіз:
   - **Жаңартулардың көздері**

     Тарату нүктелері үшін жаңарту көзі ретінде келесі ресурстарды пайдалануға болады:
     - Kaspersky жаңарту серверлері

Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

Әдепкі бойынша, осы нұсқа таңдалады.

- Жергілікті немесе желілік қалта

  Соңғы жаңартуларды қамтитын жергілікті немесе желілік қалта. Желілік қалта FTP сервері, HTTP сервері немесе SMB жалпы ресурсы болуы мүмкін. Желілік қалта түпнұсқалықты тексеруді қажет етсе, тек SMB протоколына қолдау көрсетіледі. Жергілікті қалтаны таңдағанда, Басқару сервері орнатылған құрылғыдағы қалтаны көрсету қажет.

  > Жаңарту көзі ретінде пайдаланылатын FTP серверінде, HTTP серверінде немесе желілік қалтада Kaspersky жаңарту серверлерін пайдалану кезінде жасалған қалталар құрылымына сәйкес келетін қалталар құрылымы (жаңартулармен бірге) болуы керек.

- **Жаңартулар сақталатын қалта**

  Сақталған жаңартуларды сақтау үшін көрсетілген қалтаға апаратын жол. Көрсетілген қалтаға апаратын жолды алмасу буферіне көшіруге болады. Топтық тапсырма үшін көрсетілген қалтаға апаратын жолды өзгерте алмайсыз.

- **diff файлдарды жүктеп алу**

  Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

  Әдепкі бойынша, параметр өшірулі.

- **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу**

  14-ші нұсқадан бастап, Kaspersky Security Center бағдарламасы дерекқорлар мен бағдарлама модульдері жаңартуларын жаңа схема бойынша жүктеп алады. Бағдарлама жаңартуларды жаңа схеманың көмегімен жүктей алуы үшін, жаңарту көзі жаңа схемамен үйлесімді метадеректері бар жаңарту файлдарын қамтуы керек. Жаңарту көзінде тек ескі схемамен үйлесімді метадеректері бар жаңарту файлдары болса, **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз. Әйтпесе, жаңартуларды жүктеу тапсырмасы қатемен аяқталады.

  Мысалы, жаңарту көзі ретінде жергілікті немесе желілік қалта көрсетілсе және осы қалтадағы жаңарту файлдары келесі бағдарламалардың бірімен жүктелген болса, осы параметрді қосу керек:

  - Kaspersky Update Utility

    Бұл утилита жаңартуларды ескі схема бойынша жүктейді.

  - Kaspersky Security Center 13.2 немесе одан бұрынғы нұсқасы

    Мысалы, тарату нүктесі жергілікті немесе желілік қалтадан жаңартуларды алу үшін конфигурацияланған. Бұл жағдайда, сіз интернетке қосылған Басқару серверін пайдалану арқылы жаңартуларды жүктей аласыз, содан кейін жаңартуларды тарату нүктесіндегі жергілікті қалтаға орналастыра аласыз. Басқару сервері нұсқасының нөмірі 13.2 немесе одан төмен болса, *Тарату нүктелерінің қоймаларына жаңартуларды жүктеу* тапсырмасында **Ескі схеманы пайдаланып, жаңартуларды жүктеп алу** параметрін қосыңыз.

  Әдепкі бойынша, параметр өшірулі.

10. Тапсырманы іске қосу кестесін жасаңыз. Қажет болса, келесі параметрлерді конфигурациялаңыз:

- **Тапсырманы бастау**

  Тапсырма орындалатын кестені таңдап, таңдалған кестені конфигурациялаңыз.

  - **Қолмен**

    Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

    Әдепкі бойынша, осы нұсқа таңдалған.

  - **N минут сайын**

    Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

  - **N сағат сайын**

    Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

  - **N күн сайын**

    Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

    Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

  - **Апта күндері бойынша**

    Тапсырма жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

    Әдепкі бойынша, тапсырма жұма сайын, сағат 18:00:00-де іске қосылады.

  - **Ай сайын**

    Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

    Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

    Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

  - **Ай сайын, таңдалған апталардың көрсетілген күндері**

    Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

    Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

    > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

    Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

  Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

11. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Тапсырманы жасау кезінде көрсетілетін параметрлерге қосымша ретінде, сіз осы тапсырманың басқа параметрлерін өзгерте аласыз.

Жаңартуларды тарату орындарының қоймаларына жүктеп алу тапсырмасын орындау нәтижесінде, дерекқорлар мен бағдарламалық модульдердің жаңартулары жаңарту көзінен көшіріледі және ортақ қатынасы бар қалтаға орналастырылады. Жүктелген жаңартуларды тек көрсетілген басқару тобына кіретін және жаңартуларды алу үшін нақты белгіленген тапсырмасы жоқ тарату нүктелері ғана пайдаланады.

Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды қосу және өшіру

Басқару серверіне арналған жаңартулар мен патчтарды әкімші нақты мақұлдағаннан кейін ғана орнатуға болады.

Kaspersky Security Center құрамдастарына арналған жаңартуларды автоматты түрде орнату құрылғыға Желілік агент орнатылған кезде әдепкі бойынша қосылады. Сіз оны Желілік агент орнатқан кезде өшіре аласыз немесе кейінірек саясаттың көмегімен өшіре аласыз.

Құрылғыға Желілік агентті жергілікті түрде орнатқан кезде Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнатуды өшіру:

1. Желілік агентті құрылғыға жергілікті түрде орнатуды іске қосыңыз.
2. **Қосымша параметрлер** қадамында **"Анықталмаған" күйі бар Kaspersky Security Center құрамдастары үшін қолжетімді жаңартулар мен патчтерді автоматты түрде орнату** жалаушасын алып тастаңыз.
3. Содан кейін, шебердің нұсқауларын орындаңыз.

Құрылғыға Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату өшірулі Желілік агент орнатылады. Автоматты орнатуды кейінірек саясаттың көмегімен қосуға болады.

Орнату пакетін пайдалану арқылы құрылғыға Желілік агент орнатқан кезде Kaspersky Security Center құрамдастарына арналған жаңартуларды автоматты түрде орнатуды өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Қоймалар** → **Орнату пакеттері** бөліміне өтіңіз.
2. **Kaspersky Security Center Желілік агенті <нұсқа нөмірі>** пакетін басыңыз.
3. Сипаттар терезесінде **Параметрлер** қойыншасын ашыңыз.
4. **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату** қосқышын өшіріңіз.

   Басқару агенті, Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату мүмкіндігі өшірулі болып табылатын осы пакеттен орнатылады. Автоматты орнатуды кейінірек саясаттың көмегімен қосуға болады.

Желілік агентті құрылғыға орнатқан кезде жалауша қойылса (алынып тасталса), кейіннен Желілік агент саясатын пайдалану арқылы автоматты түрде орнатуды өшіруге (қосуға) болады.

Желілік агент саясатын қолдану арқылы Kaspersky Security Center құрамдастарына арналған жаңартулар мен патчтарды автоматты түрде орнатуды қосу немесе өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. Желілік агент саясатын басыңыз.
3. Саясат сипаттары терезесінде **Бағдарлама параметрлері** қойыншасын ашыңыз.
4. **Патчтарды және жаңартуларды басқару** бөлімінде, жаңартулар мен патчтарды автоматты түрде орнатуды қосу немесе өшіру үшін **Белгісіз күйге ие компоненттер үшін қолданылатын жаңартулар мен патчтарды автоматты түрде орнату** қосқышын қосыңыз немесе өшіріңіз.
5. Осы қосқыш үшін белгішені (🔒) орнатыңыз.

   Саясат таңдалған құрылғыларға қолданылады, ал Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату осы құрылғыларда қосылады (өшіріледі).

Kaspersky Endpoint Security for Windows жаңартуларын автоматты түрде орнату

Клиент құрылғыларында Kaspersky Endpoint Security for Windows бағдарламасының дерекқорлары мен модульдерін автоматты түрде жаңартуды конфигурациялауға болады.

Kaspersky Endpoint Security for Windows жаңартуларын құрылғыларға жүктеуді және автоматты түрде орнатуды конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Kaspersky Endpoint Security for Windows бағдарламасы үшін **Жаңарту** тапсырмасы ішкі түрін таңдаңыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

5. Тапсырманың әрекет ету ауқымын таңдаңыз.

6. Тапсырма қолданылатын басқару тобын, құрылғылар немесе құрылғы таңдауын көрсетіңіз.

7. **Тапсырманы жасауды аяқтау** қадамында, әдепкі бойынша тапсырма параметрлерін өзгерткіңіз келсе, **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосыңыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

8. **Жасау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

9. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

10. Жаңарту тапсырмасы сипаттары терезесінде, **Бағдарлама параметрлері** қойыншасында жергілікті немесе ұялы режимді көрсетіңіз:

    - **Жергілікті режим**: құрылғы мен Басқару сервері арасында байланыс орнатылған.
    - **Ұялы режим**: құрылғы мен Kaspersky Security Center арасында байланыс орнатылмаған (мысалы, құрылғы интернетке қосылмаған болса).

11. Kaspersky Endpoint Security for Windows бағдарламасының дерекқорлары мен модульдерін жаңарту үшін пайдаланғыңыз келетін жаңарту көздерін қосыңыз. Тізімдегі жаңарту көздерінің орнын өзгерту қажет болса, **Жоғары жылжыту** және **Төменге жылжыту** түймелерін пайдаланыңыз. Бірнеше жаңарту көздері қосылған болса, Kaspersky Endpoint Security for Windows бағдарламасы оларға бір-бірлеп, тізімнің жоғарғы жағынан бастап қосылуға тырысады және бірінші қолжетімді көзден жаңарту пакетін алып шығару арқылы жаңарту тапсырмасын орындайды.

12. Бағдарлама модульдерінің жаңартуларын бағдарлама дерекқорларымен бірге жүктеу және орнату үшін **Бағдарлама модульдерінің жаңартуларын орнату** параметрін қосыңыз.

    Егер параметр қосулы болса, Kaspersky Endpoint Security for Windows бағдарламасы пайдаланушыға бағдарлама модульдерінің қолжетімді жаңартулары туралы хабарлайды және жаңарту тапсырмасы орындалған кезде бағдарлама модульдерінің жаңартуларын жаңарту пакетіне қосады. Kaspersky Endpoint Security for Windows бағдарламасы тек сіз *Расталды* күйін орнатқан жаңартуларды орнатады; жаңартулар бағдарлама интерфейсі арқылы немесе Kaspersky Security Center арқылы жергілікті түрде орнатылады.

    Сондай-ақ, **Бағдарлама модулінің критикалық жаңартуларын автоматты түрде орнату** параметрін қосуға да болады. Бағдарлама модульдерінің жаңартулары болған кезде, Kaspersky Endpoint Security for Windows бағдарламасы *Критикалық* күйі бар жаңартуларды автоматты түрде орнатады; бағдарлама модульдерінің қалған жаңартуларын – әкімші оларды орнатуды мақұлдағаннан кейін.

    Егер бағдарлама модульдерін жаңарту Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен танысуды және келісуді көздейтін болса, онда пайдаланушы Лицензиялық келісімнің және Құпиялылық саясатының ережелерімен келіскеннен кейін, бағдарлама жаңартуды белгілейді.

13. Бағдарлама жүктелген жаңартуларды қалтаға сақтайтын **Жаңартуларды қалтаға көшіру** жалаушасын қойыңыз, содан кейін қалта жолын көрсетіңіз.

14. Тапсырманы бастау кестесін белгілеңіз. Уақтылы жаңартуды қамтамасыз ету үшін, **Қоймаға жаңартуларды жүктеу кезінде** нұсқасын таңдау ұсынылады.

15. **Сақтау** түймесін басыңыз.

> **Жаңарту** тапсырмасын орындау кезінде, бағдарлама Kaspersky жаңартулар серверлеріне сұрау салады.

> Кейбір жаңартулар басқарылатын бағдарлама плагиндерінің соңғы нұсқаларын орнатуды талап етеді.

Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау

Жаңартуларды орнату тапсырмасының параметрлері, орнатылуы тиісті жаңартуларды мақұлдауды талап етуі мүмкін. Орнату қажет болған жаңартуларды растай аласыз немесе орнатылмауы тиісті жаңартулардан бас тарта аласыз.

Мысалы, сіз алдымен жаңартуларды сынақ ортасында орнатуды тексеріп, олар құрылғылардың жұмысына кедергі келтірмейтіндігіне көз жеткізіп алып, содан кейін осы жаңартуларды клиент құрылғыларына орната аласыз.

> Жаңартуларды мақұлдау және қабылдамау Windows жүйесінде орнатылған клиенттік құрылғыларда орнатылған Желілік агент және басқарылатын қолданбалар үшін ғана қолжетімді. Басқару серверін, Kaspersky Security Center Web Console веб-консолін және веб-басқару плагиндерін үздіксіз жаңартуға қолдау көрсетілмейді. Бұл компоненттерді жаңарту үшін, олардың соңғы нұсқаларын Kaspersky сайтынан жүктеп алу және қолмен орнату керек.

Бір немесе бірнеше жаңартуды растау немесе болдырмау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Kaspersky бағдарламалары** → **Байқалмайтын жаңартулар** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

   > Басқарылатын бағдарламаларды жаңарту үшін Kaspersky Security Center бағдарламасының белгілі бір ықшам нұсқасын орнату қажет болуы мүмкін. Бұл нұсқа сіздің қазіргі нұсқаңыздан да соңғы болса, бұл жаңартулар көрсетілсе де, оларды мақұлдау мүмкін емес. Сондай-ақ, Kaspersky Security Center жаңартпайынша, осындай жаңартулардан орнату пакеттерін жасау мүмкін емес. Сізге Kaspersky Security Center данасын қажетті ықшам нұсқаға дейін жаңарту ұсынылады.

2. Растау немесе қабылдамау қажет болған жаңартуларды таңдаңыз.

3. Таңдалған жаңартуды мақұлдау үшін **Бекіту** түймесін басыңыз немесе таңдалған жаңартуды қабылдамау үшін **Қабылдамау** түймесін басыңыз.

   Әдепкі бойынша, *Анықталмаған* мәні орнатылған.

Расталды күйі белгіленген жаңартулар орнатуға кезекке қойылады.

Қабылданбады күйі белгіленген жаңартулар, бұған дейін орнатылған құрылғылардан жойылады (бұл мүмкін болса). Сондай-ақ, олар құрылғыларға кейінірек орнатылмайды.

Kaspersky бағдарламаларына арналған жаңартулардың кейбірін жою мүмкін емес. Оларға *Қабылданбады* күйін белгілеген болсаңыз, Kaspersky Security Center бағдарламасы осы жаңартуларды бұған дейін орнатылған құрылғылардан жоймайды. Мұндай жаңартулар болашақта құрылғыларға ешқашан орнатылмайды.

Үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін *Қабылданбады* күйін белгілеп жатсаңыз, бұл жаңартулар орнатылуы жоспарланған, бірақ әлі орнатылмаған құрылғыларға орнатылмайды. Жаңартулар әлдеқашан орнатылған құрылғыларда қала береді. Жаңартуларды жою қажет болса, мұны жергілікті түрде қолмен орындай аласыз.

Басқару серверін жаңарту

Басқару серверін жаңарту шебері көмегімен Басқару серверінің жаңартуларын орнатуға болады.

Басқару серверінің жаңартуларын орнату үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Kaspersky бағдарламалары → Байқалмайтын жаңартулар** бөліміне өтіңіз.

2. Басқару серверін жаңарту шебері процесін келесі тәсілдердің бірімен іске қосыңыз:

   - Жаңартулар тізіміндегі Басқару сервері жаңартуының атын басып, ашылған терезеде **Басқару серверін жаңарту шеберін іске қосу** сілтемесінен өтіңіз.

   - Бағдарлама терезесінің жоғарғы жағындағы хабарландыру өрісінде **Басқару серверін жаңарту шеберін іске қосу** сілтемесінен өтіңіз.

3. Жаңартуды қашан орнату керектігін көрсету үшін Басқару серверін жаңарту шебері терезесінде келесі нұсқалардың бірін таңдаңыз:

   - **Қазір орнату**. Жаңартуларды қазір орнатқыңыз келсе, осы нұсқаны таңдаңыз.

   - **Орнатуды кейінге қалдыру**. Жаңартуларды кейінірек орнатқыңыз келсе, осы нұсқаны таңдаңыз. Бұл жағдайда, осы жаңарту туралы хабарландыру көрсетіледі.

   - **Осы жаңартуды елемеу**. Жаңартуды орнатқыңыз келмесе және осы жаңарту туралы хабарландыру алғыңыз келмесе, осы нұсқаны таңдаңыз.

4. Жаңартуды орнатпас бұрын Басқару серверінің сақтық көшірмесін жасағыңыз келсе, **Жаңартуды орнату алдында Басқару серверінің сақтық көшірмесін жасау** параметрін таңдаңыз.

5. Шебер терезесін жабу үшін **OK** түймесін басыңыз.

Сақтық көшірмелеу процесінде жаңартуларды орнату процесі үзіледі.

Жаңартуларды алудың офлайн-моделін қосу және өшіру

Жаңартуларды алудың офлайн-моделін өшіру ұсынылмайды. Өшіру салдарынан құрылғыларға жаңартуларды жеткізу кезінде ақау туындауы мүмкін. Кейбір жағдайларда, Kaspersky техникалық қолдау қызметінің мамандары сізге **Басқару серверінен жаңартулар мен антивирустық дерекқорларды алдын ала жүктеп алу** параметрін өшіруді ұсынуы мүмкін. Олай болса, Kaspersky бағдарламалары үшін қоймаларға жаңартуларды жүктеу тапсырмасы конфигурацияланғанына көз жеткізуіңіз керек.

Басқару тобына арналған жаңартуларды алудың офлайн-моделін қосу немесе өшіру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.
2. **Топтар** түймесін басыңыз.
3. Басқару топтары тізімінде, жаңартуларды алудың офлайн-моделі қосылуы қажет басқару тобын таңдаңыз.
4. Желілік агент саясатын басыңыз.

   Желілік агент саясатының сипаттары терезесі ашылады.

   Әдепкі бойынша, еншілес саясат параметрлері тектік саясат параметрлерін иеленеді және өзгертіле алмайды. Егер сіз өзгерткіңіз келетін саясат иеленген болса, сізге қажет басқару тобында Желілік агент үшін саясат құру қажет. Жасалған саясатта, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.
5. **Бағдарлама параметрлері** терезесінде **Патчтарды және жаңартуларды басқару** бөлімін таңдаңыз.
6. Жаңартуларды алудың офлайн-моделін қосу немесе өшіру үшін **Басқару серверінен жаңартулар мен антивирустық дерекқорды алдын ала жүктеп алыңыз (ұсынылған)** параметрін қосыңыз немесе өшіріңіз.

   Әдепкі бойынша, жаңартуларды алудың офлайн-моделі қосулы.

Соның нәтижесінде, жаңартуларды алудың офлайн-моделі қосулы немесе өшірулі болады.

Автономды құрылғыларда Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар

Басқарылатын құрылғыларда Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдеріне арналған жаңартулар, құрылғыларды вирустар мен басқа да қауіптерден қорғауды қамтамасыз етуге арналған маңызды тапсырма болып табылады. Әкімші Басқару сервері қоймасының немесе тарату нүктелері қоймасының көмегімен тұрақты жаңартуды конфигурациялайды.

Басқару серверіне (негізгі немесе қосалқы), тарату нүктесіне немесе интернетке қосылмаған құрылғыдағы (немесе құрылғылар тобындағы) дерекқорлар мен бағдарламалық модульдерді жаңарту қажет болғанда, FTP сервері немесе жергілікті қалта сияқты баламалы жаңарту көздерін пайдалану керек. Бұл жағдайда, флеш-дискі немесе сыртқы қатты диск сияқты жаппай сақтау құрылғысы арқылы қажетті жаңартулар файлдарын жеткізу керек.

Қажетті жаңартуларды осыдан көшіруге болады:

- Басқару сервері.

  Басқару сервері қоймасында автономды құрылғыда орнатылған қауіпсіздік бағдарламасына қажетті жаңартулар болуы үшін, басқарылатын желілік құрылғылардың кем дегенде біреуінде осы қауіпсіздік бағдарламасы орнатылуы керек. Бұл бағдарлама Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасы арқылы Басқару сервері қоймасынан жаңартуларды алу үшін конфигурациялануы керек.

- Бірдей қауіпсіздік бағдарламасы орнатылған және Басқару сервері қоймасынан, тарату нүктесі қоймасынан немесе тікелей Kaspersky жаңарту серверлерінен жаңартулар алуға конфигурацияланған кез келген құрылғы.

Төменде Басқару сервері қоймасынан көшіру арқылы дерекқорлар мен бағдарламалық модульдер жаңартуларын орнатудың мысалы келтірілген.

Автономды құрылғылардағы Kaspersky дерекқоры мен бағдарламалық модульдерін жаңарту үшін:

1. Алынбалы жетекті Басқару сервері орнатылған құрылғыға қосыңыз.

2. Жаңарту файлдарын алынбалы жетекке көшіріңіз.

   Жаңартулар әдепкі бойынша мына мекенжайда орналасқан: \\<сервер атауы>\KLSHARE\Updates.

   Сондай-ақ, сіз Kaspersky Security Center бағдарламасында жаңартуларды өзіңіз таңдаған қалтаға үнемі көшіруді конфигурациялай аласыз. Бұл үшін, Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасының сипаттарында **Алынған жаңартуларды қосымша қалталарға көшіру** параметрін қолданыңыз. Егер сіз жаппай сақтау құрылғысында немесе сыртқы қатты дискіде орналасқан қалтаны осы параметрдің мақсатты қалтасы ретінде көрсетсеңіз, бұл жаппай сақтау құрылғысында әрқашан жаңартулардың соңғы нұсқасы болады.

3. Автономды құрылғыларда жергілікті қалтадан немесе FTP сервері немесе ортақ қатынасы бар қалта сияқты ортақ ресурстан жаңартуларды алу үшін қауіпсіздік бағдарламасын конфигурациялаңыз (мысалы, Kaspersky Endpoint Security for Windows орнатыңыз).

4. Жаңарту файлдарын алынбалы жетектен жергілікті қалтаға немесе жаңартулар көзі ретінде пайдаланғыңыз келетін ортақ ресурсқа көшіріңіз.

5. Жаңартуларды орнатуды қажет ететін автономды құрылғыда Kaspersky Endpoint Security for Windows жаңарту тапсырмасын іске қосыңыз.

Жаңарту тапсырмасы аяқталғаннан кейін, Kaspersky дерекқорлары мен бағдарламалық модульдері құрылғыда жаңартылады.

Веб-плагиндерді сақтық көшірмелеу және қалпына келтіру

Kaspersky Security Center Web Console веб-консолі сізге сақталған күйді қалпына келтіру үшін веб-плагиннің ағымдағы күйінің деректерін сақтық көшірмелеуге мүмкіндік береді. Мысалы, веб-плагин деректерін жаңа нұсқаға жаңартпас бұрын, оның сақтық көшірмесін жасауға болады. Жаңартудан кейін, егер ең жаңа нұсқа сіздің талаптарыңызға немесе дәмелеріңізге сәйкес келмесе, деректердің сақтық көшірмесінен веб-плагиннің алдыңғы нұсқасын қалпына келтіруге болады.

Веб-плагин деректерінің сақтық көшірмесін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Параметрлер** → **Веб-плагиндер** бөліміне өтіңіз.
2. **Веб-плагиндер** бөлімінде деректердің сақтық көшірмесін жасау қажет веб-плагиндерді таңдап, **Сақтық көшірмені жасау** түймесін басыңыз.

Таңдалған веб-плагиндердің деректерін сақтық көшірмелеу. Сіз деректердің жасалған сақтық көшірмелерін **Резервтік қоймалар** қойыншасында қарап шыға аласыз.

Деректердің сақтық көшірмесінен веб-плагинді қалпына келтіру үшін:

1. Бағдарламаның негізгі терезесінде **Параметрлер** → **Резервтік қоймалар** бөліміне өтіңіз.
2. **Резервтік қоймалар** бөлімінде қалпына келтіргіңіз келетін веб-плагин деректерінің сақтық көшірмесін таңдаңыз, содан соң **Сақтық көшірмеден қалпына келтіру** түймесін басыңыз.

Веб-плагин таңдалған деректердің сақтық көшірмесінен қалпына келтіріледі.

Тарату нүктелері мен қосылым шлюздерін конфигурациялау

Kaspersky Security Center-дегі басқару топтарының құрылымы келесі функцияларды орындайды:

- Саясаттардың әрекет ету ауқымын белгілеу.

  Саясат профильдерінің көмегімен құрылғыларда параметрлердің сыртқы жиынтықтарын қолданудың баламалы тәсілі бар. Бұл жағдайда, саясаттардың әрекет ету ауқымы тегтер, құрылғылардың Active Directory ұйымдық бөлімшесінде орналасқан жерлері, Active Directory қауіпсіздік топтарындағы мүшелік және т.б. арқылы белгіленеді.

- Топтық тапсырмалардың әрекет ету ауқымын белгілеу.

  Басқару топтарының иерархиясына негізделмеген топтық тапсырмалардың әрекет ету ауқымын белгілеу тәсілдемесі бар: құрылғыларды таңдау және арнайы құрылғылар үшін тапсырмаларды қолдану.

- Құрылғыларға, виртуалды және қосалқы Басқару серверлеріне қатынасу құқықтарын белгілеу.

- Тарату нүктелерін тағайындау.

Басқару топтарының құрылымын құру кезінде тарату нүктелерін оңтайлы түрде тағайындау үшін ұйым желісінің топологиясын ескеру қажет. Тарату нүктелерінің оңтайлы таралуы арқасында ұйым желісіндегі желілік трафикті азайтуға мүмкіндік беріледі.

Ұйымның ұйымдық құрылымына және желілер топологиясына байланысты, басқару топтары құрылымының келесі типтік конфигурацияларын ажыратуға болады:

- Бір кеңсе
- Көптеген шағын оқшауланған кеңселер

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Тарату нүктелерінің типтік конфигурациясы: бір кеңсе

"Бір кеңсе" типтік конфигурациясында барлық құрылғылар ұйымның желісінде орналаса отырып, бір-бірін "көреді". Ұйымның желісі тар арналармен байланысқан бірнеше бөлектенген бөліктен (желіден немесе желі сегменттерінен) құралуы мүмкін.

Басқару топтарының құрылымын құрудың келесі тәсілдері болуы мүмкін:

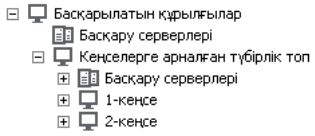
- Желі топологиясын ескере отырып, басқару тобының құрылымын құру. Басқару топтарының құрылымы желінің топологиясын нақты түрде көрсетуге міндетті емес. Желінің бөлектенген бөліктеріне қандай да бір басқару топтарының сай келуі жеткілікті. Тарату нүктелерін автоматты түрде тағайындауды қолдануға немесе тарату нүктелерін қолмен тағайындауға болады.

- Желінің топологиясын білдірмейтін басқару топтарының құрылымын құру. Бұл жағдайда, тарату нүктелерін автоматты түрде тағайындауды өшіру және желінің әрбір бөлектенген бөлігінде түбірлік басқару тобына, мысалы, **Басқарылатын құрылғылар** тобына бір немесе бірнеше құрылғыны тарату нүктелері ретінде тағайындау керек. Барлық тарату нүктелері бір деңгейде болады және бірдей "ұйым желісінің барлық құрылғылары" әрекет ету ауқымына ие болады. Желілік агенттердің әрқайсысы, бағыты ең қысқа болып саналатын тарату нүктесіне қосылатын болады. Тарату нүктесіне апаратын бағытты tracert утилитасының көмегімен анықтауға болады.

Тарату нүктелерінің типтік конфигурациясы: қашықтағы көптеген шағын кеңселер

Бұл типтік конфигурация, бәлкім, басты кеңсемен интернет арқылы байланысқан көптеген шағын қашықтағы кеңселерге сәйкес келеді. Қашықтағы кеңселердің әрқайсысы NAT артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес – кеңселер бір-бірінен оқшауланған.

Конфигурация басқару топтарының құрылымында міндетті түрде көрсетілуі керек: қашықтағы кеңселердің әрқайсысы үшін жеке басқару тобын құру керек (төмендегі суреттегі **1-кеңсе**, **2-кеңсе** топтары).



Қашықтағы кеңселер басқару топтарының құрылымында көрсетілген

Кеңсеге сай келетін әрбір басқару тобына бір немесе бірнеше тарату нүктесін тағайындау керек. Дискіде жеткілікті орны бар қашықтағы кеңсе құрылғыларын тарату нүктелері ретінде тағайындау керек. Мысалы, **1-кеңсе** тобында орналастырылған құрылғылар **1-кеңсе** басқару тобына тағайындалған тарату нүктелеріне жүгінетін болады.

Егер кейбір пайдаланушылар ноутбуктері бар кеңселер арасында физикалық түрде жылжытылатын болса, әр қашықтағы кеңседе жоғарыда аталған тарату нүктелеріне тағы екі және немесе одан да көп құрылғыны таңдап, оларды жоғарғы деңгейдегі басқару тобына тарату нүктелері ретінде тағайындау керек (жоғарыдағы суреттегі **Кеңселерге арналған түбірлік топ** тобы).

1-кеңсе басқару тобында болған, бірақ физикалық түрде **2-кеңсе** тобына сәйкес келетін кеңсеге көшірілген ноутбук. Жылжытқаннан кейін, ноутбуктағы Желілік агент **1-кеңсе** тобына тағайындалған тарату нүктелеріне жүгінуге тырысатын болады, бірақ бұл тарату нүктелері қолжетімді болмайды. Сонда Желілік агент **Кеңселерге арналған түбірлік топ** тобына тағайындалған тарату нүктелеріне жүгіне бастайды. Қашықтағы кеңселер бір-бірінен алшақ орналасқандықтан, **Кеңселерге арналған түбірлік топ** басқару тобына тағайындалған барлық тарату нүктелерінен **2-кеңсе** тобына тағайындалған тарату нүктелеріне жүгіну ғана сәтті болады. Яғни, ноутбук өзінің бастапқы кеңсесіне сәйкес келетін басқару тобында бола отырып, қазіргі уақытта физикалық түрде орналасқан кеңсенің тарату нүктесін қолдана беретін болады.

Тарату нүктелерін тағайындау туралы

Сіз басқарылатын құрылғыны тарату нүктесі ретінде қолмен немесе автоматты түрде тағайындай аласыз.

Егер сіз басқарылатын құрылғыны тарату нүктесі ретінде қолмен тағайындасаңыз, сіз өз желіңіздегі кез келген құрылғыны таңдай аласыз.

Егер сіз тарату нүктелерін автоматты түрде тағайындасаңыз, Kaspersky Security Center бағдарламасы тек келесі шарттарға сай келетін басқарылатын құрылғыларды ғана таңдай алады:

- Құрылғының дискінде кемінде 50 ГБ бос орын болуы тиіс.
- Басқарылатын құрылғы Kaspersky Security Center бағдарламасына тікелей (шлюз арқылы емес) қосылады.
- Басқарылатын құрылғы ноутбук емес.

> Сіздің желіңізде белгіленген шарттарға сай келетін құрылғылар болмаса, Kaspersky Security Center бағдарламасы қандай да бір құрылғыны тарату нүктесі етіп автоматты түрде тағайындамайды.

Тарату нүктелерін автоматты түрде тағайындау

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Бұл жағдайда, Kaspersky Security Center бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды.

> Microsoft Windows жүйесінде Arm жүйесінде жұмыс істейтін құрылғылар тарату нүктелері ретінде қызмет ете алмайды.

Тарату нүктелерін автоматты түрде тағайындау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. **Тарату нүктелерін автоматты түрде тағайындау** параметрін таңдаңыз.

   Егер тарату нүктелерінің құрылғыларын автоматты түрде тағайындау қосулы болса, тарату нүктелерінің параметрлерін қолмен конфигурациялау, сондай-ақ тарату нүктелерінің тізімін өзгерту мүмкін емес.

4. **Сақтау** түймесін басыңыз.

Нәтижесінде, Басқару сервері тарату нүктелерін автоматты түрде тағайындайды және олардың параметрлерін конфигурациялайды.

Тарату нүктелерін қолмен тағайындау

Kaspersky Security Center құрылғыларды тарату нүктелеріне қолмен тағайындауға мүмкіндік береді.

Тарату нүктелерін автоматты түрде тағайындау ұсынылады. Бұл жағдайда, Kaspersky Security Center бағдарламасы тарату нүктелеріне қандай құрылғыларды тағайындау керектігін өзі таңдайды. Алайда, егер сіз қандай да бір себептермен тарату нүктелерін автоматты түрде тағайындаудан бас тартқыңыз келсе (мысалы, арнайы бөлінген серверлерді пайдаланғыңыз келсе), Тарату нүктелерінің саны мен конфигурациясын алдын ала есептеу арқылы оларды қолмен тағайындауға болады.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Microsoft Windows жүйесінде Arm жүйесінде жұмыс істейтін құрылғылар тарату нүктелері ретінде қызмет ете алмайды.

Құрылғыны қолмен тарату нүктесі етіп тағайындау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.

3. **Тарату нүктелерін қолмен тағайындау** параметрін таңдаңыз.

4. **Белгілеу** түймесін басыңыз.

5. Тарату нүктесі етіп жасағыңыз келетін құрылғыны таңдаңыз.

   Құрылғыны таңдау кезінде тарату нүктелерінің жұмысының ерекшеліктерін және тарату нүктесінің рөлін атқаратын құрылғыға қойылатын талаптарды ескеріңіз.

6. Таңдалған тарату нүктесінің әрекет ету ауқымына қосқыңыз келетін басқару тобын таңдаңыз.

7. **ОК** түймесін басыңыз.

   Қосылған тарату нүктесі **Тарату нүктелері** бөліміндегі тарату нүктелерінің тізімінде пайда болады

8. Оның сипаттары терезесін ашу үшін тізімдегі қосылған тарату нүктесін басыңыз.

9. Сипаттар терезесінде тарату нүктесінің параметрлерін конфигурациялаңыз:

- **Жалпы** бөлімінде тарату нүктесінің клиент құрылғыларымен өзара әрекеттесу параметрін көрсетіңіз:

  - **SSL порты**

    SSL протоколын қолдана отырып, клиент құрылғыларының тарату нүктесіне қауіпсіз қосылу жүзеге асырылатын SSL портының нөмірі.

    Әдепкі бойынша порт нөмірі – 13000.

  - **Көп мекенжайлық жіберуді пайдалану**

    Егер параметр қосулы болса, орнату пакеттерін топ шегіндегі клиент құрылғыларына автоматты түрде тарату үшін көп мекенжайлы IP таратылымы қолданылады.

    Көп мекенжайлы IP таратылымы бағдарламаларды орнату пакетінен клиент құрылғылары тобына орнатуға кететін уақытты азайтады, бірақ бағдарламаны бір клиент құрылғысына орнатқан кезде орнату уақытын арттырады.

  - **IP таратудың мекенжайы**

    Көп мекенжайлы таратылым орындалатын IP мекенжайы. IP мекенжайын 224.0.0.0 – 239.255.255.255 ауқымында белгілеуге болады

    Әдепкі бойынша Kaspersky Security Center бағдарламасы белгіленген диапазонда бірегей көп мекенжайлы IP таратылымының мекенжайын тағайындайды.

  - **IP тарату портының нөмірі**

    Көп мекенжайлы таратылым портының нөмірі.

    Әдепкі бойынша порт нөмірі – 15001. Басқару сервері орнатылған құрылғы тарату нүктесі ретінде көрсетілсе, онда SSL протоколы арқылы қосылу үшін әдепкі бойынша 13001-порт қолданылады.

  - **Қашықтағы құрылғылар үшін тарату нүктесінің мекенжайы**

    Қашықтағы құрылғылар тарату нүктесіне қосылатын желілік мекенжайы.

  - **Жаңартуларды тарату**

    Жаңартулар келесі көздерден басқарылатын құрылғыларға қолданылады:

    - Бұл параметр қосулы болса, бұл тарату нүктесі болады.
    - Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе Kaspersky жаңартулар серверлері.

    Егер сіз жаңартуларды тарату үшін тарату нүктелерін қолдансаңыз, трафикті үнемдей аласыз, себебі жүктеме санын азайтасыз. Сондай-ақ, Басқару серверіндегі жүктемені азайтуға және жүктемені тарату нүктелері арасында қайта бөлуге болады. Трафик пен жүктемені оңтайландыру үшін желідегі тарату нүктелерінің санын есептеп шығаруға болады.

    Егер сіз бұл параметрді өшірсеңіз, жаңарту жүктемелері мен Басқару серверіне түсетін жүктеме артуы мүмкін. Әдепкі бойынша, параметр қосулы.

- **Орнату пакеттерін тарату**

  Орнату пакеттері келесі көздерден басқарылатын құрылғыларға қолданылады:

  - Бұл параметр қосулы болса, бұл тарату нүктесі болады.
  - Егер параметр өшірулі болса, басқа тарату нүктелері, Басқару сервері немесе Kaspersky жаңартулар серверлері.

  Егер сіз орнату пакеттерін тарату үшін тарату нүктелерін қолдансаңыз, трафикті үнемдей аласыз, себебі жүктеме санын азайтасыз. Сондай-ақ, Басқару серверіндегі жүктемені азайтуға және жүктемені тарату нүктелері арасында қайта бөлуге болады. Трафик пен жүктемені оңтайландыру үшін желідегі тарату нүктелерінің санын есептеп шығаруға болады.

  Егер сіз бұл параметрді өшірсеңіз, орнату пакеттері жүктемелері мен Басқару серверіне түсетін жүктеме артуы мүмкін. Әдепкі бойынша, параметр қосулы.

- **Push-серверді іске қосу**

  Kaspersky Security Center бағдарламасында тарату нүктесі мобильді протокол арқылы басқарылатын құрылғылар үшін және Желілік агент басқаратын құрылғылар үшін push сервері ретінде жұмыс істей алады. Мысалы, егер сіз KasperskyOS орнатылған құрылғыларды Басқару серверімен мәжбүрлеп синхрондауды қосқыңыз келсе, push сервері қосулы болуы керек. Push серверінде, push сервері қосылған тарату нүктесімен бірдей басқарылатын құрылғылар аймағы бар. Егер сізде бір басқару тобына тағайындалған бірнеше тарату нүктелері болса, олардың әрқайсысында ескерту серверін қосуға болады. Бұл жағдайда, Басқару сервері жүктемені тарату нүктелері арасында бөледі.

- **Push-серверінің порты**

  Push серверінің порт нөмірі. Сіз кез келген бос порттың нөмірін көрсете аласыз.

- **Әрекет ету ауқымы** бөлімінде тарату нүктесі жаңартуларды тарататын аймақты көрсетіңіз (басқару топтары және/немесе желілік орындар).

  > Тек Windows операциялық жүйесі жұмыс істейтін құрылғылар өздерінің желілік орындарын анықтай алады. Желілік орынды анықтау басқа операциялық жүйелермен жұмыс істейтін құрылғылар үшін қолжетімді емес.

- Егер тарату нүктесі Басқару серверінен басқа құрылғыда жұмыс істеп тұрса, **Жаңартулар көзі** бөлімінде тарату нүктесі үшін жаңартулар көзін таңдауға болады:

  - **Жаңартулар көзі**

    Тарату нүктесі үшін жаңартулар көзін таңдаңыз:

    - Тарату нүктесі Басқару серверінен жаңартулар алып тұруы үшін, **Басқару серверінен шығарып алу** нұсқасын таңдаңыз.
    - Тарату нүктесіне тапсырма арқылы жаңартуларды алуға рұқсат беру үшін, **Жаңартуды жүктеп алу тапсырмасын пайдалану** тармағын таңдаңыз және *Жаңартуларды тарату нүктелерінің қоймаларына жүктеу* тапсырмасын көрсетіңіз:
      - Егер мұндай тапсырма құрылғы үшін бұрыннан бар болса, тізімнен тапсырманы таңдаңыз.
      - Егер құрылғы үшін мұндай тапсырма әлі болмаса, тапсырманы жасау үшін **Тапсырма жасау** сілтемесінен өтіңіз. Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

- **diff файлдарды жүктеп алу**

  Бұл параметр айырмашылық файлдарын жүктеп алу функциясын қосады.

  Әдепкі бойынша, параметр қосулы.

- Егер тарату нүктелері интернетке қосылған кезде прокси-серверді пайдаланса, **Интернетке қосылу параметрлері** ішкі бөлімінде келесі параметрлерді көрсетуге болады:

  - **Прокси-серверді пайдалану**

    Егер бұл құсбелгі таңдалса, тарату нүктелерін Kaspersky жаңарту серверлеріне қосу үшін Интернет прокси-сервері пайдаланылады. Енгізу өрістерінде прокси-серверге қосылу параметрлерін баптауға болады.

    Әдепкі бойынша, жалауша алынып тасталған.

  - **Прокси серверінің мекенжайы**

    Прокси серверінің мекенжайы.

  - **Порт нөмірі**

    Қосылым орындалатын порт нөмірі.

  - **Жергілікті мекенжайларға арналған прокси-серверді айналып өту**

    Егер параметр қосулы болса, жергілікті желідегі құрылғыларға қосылған кезде прокси сервері пайдаланылмайды.

    Әдепкі бойынша, параметр өшірулі.

  - **Прокси-сервердегі түпнұсқалық растама**

    Жалауша қойылған болса, енгізу өрістерінде прокси-сервердегі түпнұсқалық растама үшін есептік деректерді көрсетуге болады.

    Әдепкі бойынша, жалауша алынып тасталған.

  - **Пайдаланушы аты**

    Прокси-серверге қосылу орындалатын реттелетін есептік жазбасы.

  - **Құпиясөз**

    Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

- **KSN Проксиі** бөлімінде бағдарламаны тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын жіберу үшін пайдаланылатындай етіп орнатуға болады.

  - **Тарату нүктесі тарапынан KSN проксиін қосу**

    KSN прокси-сервері қызметі тарату нүктесі ретінде әрекет ететін құрылғыда орындалады. Бұл параметрді желі трафигін қайта тарату және оңтайландыру үшін пайдаланыңыз.

    Тарату нүктесі Kaspersky Security Network мәлімдемесінде көрсетілген KSN статистикасын Kaspersky ұйымына жібереді.

    Әдепкі бойынша, параметр өшірулі. Осы параметрді қосу, **Басқару серверін прокси-сервер ретінде пайдалану** және **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын** параметрлері Басқару серверінің сипаттары терезесінде қосылған жағдайда ғана күшіне енеді.

Суық резерві бар істен шығуға төзімді кластер түйініне (белсенді / пассивті) тарату нүктесін тағайындауға және сол түйінде KSN прокси-серверін қосуға болады.

- **KSN сұрауын Басқару серверіне қайта жіберу**

  Тарату нүктесі басқарылатын құрылғылардан KSN сұрауларын Басқару серверіне жібереді.

  Әдепкі бойынша, параметр қосулы.

- **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру**

  Тарату нүктесі KSN-ге басқарылатын құрылғылардан KSN немесе KPSN бұлттық қызметіне сұраулар жібереді. Тарату нүктесінде жасалған KSN сұраулары да тікелей KSN Cloud немесе KPSN-ге жіберіледі.

  Желілік агенттің 11 (немесе одан бұрынғы) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алмайды. Тарату нүктелерін KSN сұрауларын KSN-ге жіберу үшін қайта реттегіңіз келсе, әрбір тарату нүктесі үшін **KSN сұрауын Басқару серверіне қайта жіберу** параметрін қосыңыз.

  Желілік агенттің 12 (және одан да жоғары) нұсқасы орнатылған тарату нүктелері KPSN-ге тікелей жүгіне алады.

- **KPSN желісіне қосылған кезде прокси-сервер параметрлерін елемеу**

  Егер прокси-сервер параметрлері тарату нүктелерінің немесе Желілік агенттің сипаттарында конфигурацияланған болса, бірақ сіздің желіңіздің архитектурасы KPSN бағдарламасын тікелей пайдалануды талап етсе, осы жалаушаны қойыңыз. Әйтпесе, басқарылатын қолданбадан сұрау KPSN қолданбасына берілмейді.

  Бұл параметр **KSN бұлтына/KPSN бағдарламасына интернет арқылы тікелей кіру** параметрін таңдаған жағдайда қолжетімді болады.

- **Порт**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын TCP портының нөмірі. Әдепкі бойынша 13111-порт орнатылған.

- **UDP портын қолдану**

  Басқарылатын құрылғылардың KSN прокси серверіне UDP порты арқылы қосылуы үшін **UDP портын пайдалану** жалаушасын қойып, UDP порты нөмірін көрсетіңіз. Әдепкі бойынша, параметр қосулы.

- **UDP порты**

  Басқарылатын құрылғылар KSN прокси-серверіне қосылу үшін қолдана алатын UDP портының нөмірі. Әдепкі бойынша, KSN прокси-серверіне қосылу 15111 UDP порты арқылы жүзеге асырылады.

- Егер тарату нүктесі Басқару серверінен басқа құрылғыда жұмыс істеп тұрса, **Қосылым шлюзі** бөлімінде тарату нүктесін Желілік агент және Басқару сервері үлгілері үшін қосылым шлюзі ретінде конфигурациялауға болады:

  - **Қосылым шлюзі**

    Басқару сервері мен Желілік агенттер арасында тікелей байланыс желіңізді ұйымдастыруға байланысты орнатылмаса, тарату нүктесін Басқару сервері мен Желілік агенттер арасындағы қосылым шлюзі ретінде пайдалануға болады.

    Тарату нүктесінің Желілік агенттері мен Басқару сервері арасындағы қосылым шлюзі ретінде әрекет етуін қаласаңыз, бұл параметрді қосыңыз. Әдепкі бойынша, параметр өшірулі.

- **Басқару серверінің тарабынан шлюзбен байланысты орнату (шлюз DMZ режимінде болса)**

  Басқару сервері демилитаризацияланған аймақтан (DMZ) тыс жерде болса, жергілікті желіде қашықтағы құрылғыларда орнатылған Желілік агенттер Басқару серверіне қосыла алмайды. Тарату нүктесін кері қосылымы бар қосылым шлюзі ретінде пайдалануға болады (Басқару сервері тарату нүктесімен байланысты орнатады).

  Басқару серверін демилитаризацияланған аймақтағы қосылым шлюзіне қосқыңыз келсе, осы параметрді қосыңыз.

- **Kaspersky Security Center Web Console жергілікті портын ашу**

  Демилитаризацияланған аймақта немесе интернетте орналасқан Web Console портын ашу үшін демилитаризацияланған аймақта қосылым шлюзі қажет болса, бұл параметрді қосыңыз. Web Console веб-консолін тарату нүктесіне қосу үшін пайдаланылатын порт нөмірін көрсетіңіз. Әдепкі бойынша 13299-порт орнатылған.

  Бұл параметр **Басқару серверінің тарабынан шлюзбен байланысты орнату (шлюз DMZ режимінде болса)** қолжетімді болады.

Мобильді құрылғыларды Басқару серверіне қосылым шлюзі ретінде әрекет ететін тарату нүктесі арқылы қосқанда, келесі параметрлерді қосуға болады:

- **Ұялы құрылғылар үшін портты ашу (тек Басқару серверінің SSL түпнұсқалық растамасы)**

  Қосылым шлюзінің ұялы құрылғылар үшін портты ашуын қаласаңыз және ұялы құрылғылар тарату нүктесіне қосылу үшін пайдаланатын порт нөмірін көрсетсеңіз, бұл параметрді қосыңыз. Әдепкі бойынша 13292-порт орнатылған. Мобильді құрылғы Басқару сервері сертификатын тексереді. Байланыс орнатылған кезде, тек Басқару сервері түпнұсқалық растамасын орындайды.

- **Ұялы құрылғылар үшін портты ашу (екі жақты SSL түпнұсқалық растамасы)**

  Қосылым шлюзінің Басқару сервері мен ұялы құрылғылардың екі жақты түпнұсқалық растамасы үшін пайдаланылатын портты ашуын қаласаңыз, осы параметрді қосыңыз. Мобильді құрылғы Басқару сервері сертификатын, ал Басқару сервері мобильді құрылғы сертификатын тексереді. Келесі параметрлерді белгілеңіз:

  - Ұялы құрылғылар тарату нүктесіне қосылу үшін пайдаланатын порт нөмірі. Әдепкі бойынша 13293-порт орнатылған.

  - Ұялы құрылғылар пайдаланатын қосылым шлюзі DNS домені атаулары. Домен атауларын үтірмен бөліңіз. Көрсетілген домен атаулары тарату нүктесі сертификатына қосылады. Ұялы құрылғылар пайдаланатын домен атаулары тарату нүктесі сертификатындағы жалпы атауға сәйкес келмесе, ұялы құрылғылар тарату нүктесіне қосылмайды.

    Әдепкі DNS домен атауы қосылым шлюзінің толық жарамды домен атауы болып табылады.

Екі жағдайда да сертификаттар тек тарату нүктесінде TLS сеансын орнату кезінде тексеріледі. Сертификаттарды Басқару сервері тексеруге жібермейді. Мобильді құрылғымен TLS сеансын орнатқаннан кейін тарату нүктесі мобильді құрылғы мен Басқару сервері арасында синхрондау туннелін жасау үшін Басқару сервері сертификатын пайдаланады. Екі жақты SSL аутентификациясы үшін портты ашсаңыз, мобильді құрылғы сертификатын таратудың жалғыз жолы орнату бумасы арқылы жүзеге асады.

- Windows домендерінің, Active Directory және IP ауқымдарының сауалнамасын тарату нүктесі арқылы конфигурациялаңыз:

  - **Windows домендері**

    Сіз Windows домендеріне арналған құрылғыларды анықтауды қосып, оның кестесін белгілей аласыз.

- **Домен контроллері**

  Сіз Active Directory сауалнамасын қосып, сауалнама кестесін белгілей аласыз.

  Windows операциялық жүйесі бар тарату нүктесін пайдалансаңыз, келесі нұсқалардың бірін таңдауға болады:

  - **Ағымдағы Active Directory доменінде сауалнама өткізу**.
  - **Active Directory домендер тобында сауалнама өткізу**.
  - **Таңдалған Active Directory домендерінде сауалнама өткізу**. Егер сіз осы нұсқаны таңдасаңыз, тізімге бір немесе бірнеше Active Directory доменін қосыңыз.

  Желілік агенттің 15-нұсқасы орнатылған Linux операциялық жүйесімен жұмыс істейтін тарату нүктесін пайдалансаңыз, мекенжай мен пайдаланушының есептік жазба деректерін көрсеткен Active Directory домендеріне ғана сауалнама жүргізуге болады. Ағымдағы Active Directory домені мен Active Directory доменінің тобы үшін сауалнама жүргізу қолжетімді емес.

  Домен контроллері үшін құрылғыларды табу мүмкіндігін қосуға болады.

  Домен контроллері сауалнамасын қосу параметрін таңдасаңыз, сауалнама үшін домен контроллерлерін таңдап, кестені орнатуға болады.

  Linux операциялық жүйесі бар тарату нүктесін пайдалансаңыз, **Көрсетілген домендер сауалнамасын жүргізу** бөлімінде **Қосу** түймесін басып, домен контроллерінің мекенжайы мен пайдаланушының есептік жазба деректерін көрсетіңіз.

  Windows операциялық жүйесі бар тарату нүктесін пайдалансаңыз, келесі нұсқалардың бірін таңдауға болады:

  - **Ағымдағы домен сауалнамасын жүргізу**
  - **Бүкіл домендер тобының сауалнамасын жүргізу**
  - **Көрсетілген домендер сауалнамасын жүргізу**

- **IP ауқымдары**

  IPv4 ауқымдары мен IPv6 желілері үшін құрылғыларды табу функциясын қосуға болады.

  Ауқым сауалнамасын қосу параметрін қоссаңыз, сауалнама ауқымын қосып, сауалнама кестесін белгілеуге болады. IP ауқымдарын сауалнама ауқымдары тізіміне қоса аласыз.

  IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану параметрін қоссаңыз, тарату нүктесі нөлдік конфигурациясы бар желіні қолдана отырып, IPv6 желісіне сауалнама өткізеді (бұдан әрі *Zeroconf* деп те аталады). Бұл жағдайда, көрсетілген IP ауқымдары еленбейді, өйткені тарату нүктесі бүкіл желіге сауалнама өткізеді. **IPv6 желілеріне сауалнама жүргізу үшін Zeroconf пайдалану** параметрі, тарату нүктесі Linux басқаруымен жұмыс істеп тұрса қолжетімді. Zeroconf IPv6 сауалнамасын пайдалану үшін тарату нүктесінде avahi-browse утилитасын орнату қажет.

- **Кеңейтілген** бөлімінде тарату нүктесі таратылатын деректерді сақтау үшін пайдалануы керек қалтаны көрсетіңіз:

  - **Әдепкі бойынша қалтаны қолдану**

    Деректерді сақтау үшін осы нұсқаны таңдағанда, тарату нүктесінде Желілік агент орнатылған қалта қолданылады.

- **Көрсетілген қалтаны пайдалану**

  Бұл нұсқаны таңдағанда, төмендегі өрісте қалта жолын көрсетуге болады. Қалта тарату нүктесінде де, қашықтан да, ұйым желісінің құрамына кіретін кез келген құрылғыда орналастырылуы мүмкін.

  Тарату нүктесінде Желілік агент іске қосылатын есептік жазба оқу және жазу үшін көрсетілген қалтаға қатынасу мүмкіндігіне ие болуы керек.

10. **OK** түймесін басыңыз.

Нәтижесінде, таңдалған құрылғылар тарату нүктелерінің рөлін атқарады.

Басқару тобы үшін тарату нүктелерінің тізімін өзгерту

Сіз белгілі бір басқару тобына тағайындалған тарату нүктелерінің тізімін көре аласыз және тарату нүктелерін қосу немесе жою арқылы тізімді өзгерте аласыз.

Басқару тобы үшін тарату нүктелерінің тізімін қарау және өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Басқарылатын құрылғылар тізімінің үстіндегі **Ағымдағы жол** өрісінде сілтеме бойынша өтіңіз.
3. Сол жағында ашылған панельде тағайындалған тарату нүктелерін көргіңіз келетін басқару тобын таңдаңыз.

   Ол үшін **Тарату нүктелері** мәзір тармағын пайдаланыңыз.
4. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тарату нүктелері** бөліміне өтіңіз.
5. Басқару тобына тарату нүктелерін қосу үшін, басқарылатын құрылғылар тізімінің үстіндегі **Белгілеу** түймесін басыңыз және ашылатын панельде құрылғыларды таңдаңыз.
6. Тағайындалған тарату нүктелерін жою үшін тізімнен құрылғыларды таңдап, **Белгілеуден бас тарту** түймені басыңыз.

Өзгерістерге байланысты, тарату нүктелері тізімге қосылады немесе қолданыстағы тарату нүктелері тізімнен жойылады.

Мәжбүрлеп синхрондау

Kaspersky Security Center бағдарламасы басқарылатын құрылғылар үшін күйді, параметрлерді, тапсырмаларды және саясаттарды автоматты түрде синхрондайды, бірақ кейбір жағдайларда аталған құрылғы үшін синхрондауды мәжбүрлеп іске қосу қажет болуы мүмкін. Сіз мәжбүрлеп синхрондауды келесі құрылғылар үшін іске қоса аласыз:

- Желілік агенті орнатылған құрылғылар.
- KasperskyOS басқаратын құрылғылар.

  KasperskyOS басқаратын құрылғы үшін мәжбүрлеп синхрондауды іске қосар алдында, құрылғының тарату нүктесінің әрекет ету ауқымына қосылғанына және тарату нүктесінде push серверінің қосулы екеніне көз жеткізіңіз.
- iOS құрылғылары.

- Android құрылғылары.

  Android құрылғылары үшін мәжбүрлеп синхрондауды іске қосар алдында, Firebase Cloud Messaging конфигурациялау керек.

Бір құрылғыны синхрондау

Басқару сервері мен басқарылатын құрылғы арасында мәжбүрлеп синхрондауды жүзеге асыру:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Басқару серверімен синхрондау қажет құрылғының атауын таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.
3. **Мәжбүрлеп синхрондау** түймесін басыңыз.

Бағдарлама таңдалған құрылғыны Басқару серверімен синхрондауды орындайды.

Бірнеше құрылғыны синхрондау

Басқару сервері мен бірнеше басқарылатын құрылғылар арасында мәжбүрлеп синхрондауды жүзеге асыру:

1. Басқару тобы құрылғылары тізімін немесе құрылғы таңдауларын ашыңыз:

   - Негізгі мәзірде **Активтер (құрылғылар)**→ **Басқарылатын құрылғылар** бөліміне өтіңіз, басқарылатын құрылғылар тізімінің үстінде **Ағымдағы жол** өрістегі сілтемеден өтіңіз және синхрондалатын құрылғыларды қамтитын басқару тобын таңдаңыз.

   - Құрылғылар тізімін қарау үшін құрылғы таңдауларын іске қосыңыз.
2. Басқару серверімен синхрондауды қажет ететін құрылғылардың жанында жалауша қойыңыз.
3. Басқарылатын құрылғылар тізімі үстінде көп нүктелі (...) түймесін басып, **Мәжбүрлеп синхрондау** түймесін басыңыз.

   Бағдарлама таңдалған құрылғыларды Басқару серверімен синхрондауды орындайды.
4. Құрылғылар тізімінде таңдалған құрылғылар үшін соңғы Басқару серверіне қосылу уақыты ағымдағы уақытқа өзгергенін тексеріңіз. Егер уақыт өзгермесе, **Жаңарту** түймесін басу арқылы беттің мазмұнын жаңартыңыз.

Таңдалған құрылғылар Басқару серверімен синхрондалады.

Саясатты жеткізу уақытын қарау

Басқару серверіндегі Kaspersky бағдарламасының саясатын өзгерткеннен кейін, әкімші өзгертілген саясаттың белгілі бір басқарылатын құрылғыларға жеткізілгенін не жеткізілмегенін тексере алады. Саясат тұрақты немесе мәжбүрлеп синхрондау кезінде жеткізілуі мүмкін.

Басқарылатын құрылғыларға бағдарлама саясатын жеткізу күні мен уақытын көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Басқару серверімен синхрондау қажет құрылғының атауын таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.
3. **Бағдарламалар** қойындысын таңдаңыз.
4. Саясатты синхрондау күнін көру қажет бағдарламаны таңдаңыз.

   Бағдарлама саясаты терезесі **Жалпы** таңдалған бөлімімен бірге ашылады және саясаттың жеткізілу күні мен уақыты көрсетіледі.

Push серверін қосу

Kaspersky Security Center бағдарламасында тарату нүктесі мобильді протокол арқылы басқарылатын құрылғылар үшін және Желілік агент басқаратын құрылғылар үшін push сервері ретінде жұмыс істей алады. Мысалы, егер сіз KasperskyOS орнатылған құрылғыларды Басқару серверімен мәжбүрлеп синхрондауды қосқыңыз келсе, push сервері қосулы болуы керек. Push серверінде, push сервері қосылған тарату нүктесімен бірдей басқарылатын құрылғылар аймағы бар. Егер сізде бір басқару тобына тағайындалған бірнеше тарату нүктелері болса, олардың әрқайсысында ескерту серверін қосуға болады. Бұл жағдайда, Басқару сервері жүктемені тарату нүктелері арасында бөледі.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін тарату нүктелерін push серверлері ретінде пайдаланғыңыз келуі мүмкін. Тұрақты байланыс жергілікті тапсырмаларды іске қосу және тоқтату, басқарылатын бағдарламаның статистикасын алу немесе туннель жасау сияқты кейбір операциялар үшін қажет. Тарату нүктесін push серверінің сервері ретінде қолдансаңыз, сізге басқарылатын құрылғыларда **Басқару серверімен байланысты үзбеу** параметрін қолдану немесе Желілік агенттің UDP портына пакеттерді жіберу қажет емес.

Push сервері бір мезгілдегі 50 000 қосылымға дейінгі жүктемені қолдайды.

Тарату нүктесінде push серверін қосу үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.
2. **Жалпы** қойыншасында **Тарату нүктелері** бөлімін таңдаңыз.
3. Push серверін қосқыңыз келетін тарату нүктесінің атауын басыңыз.

   Тарату нүктесі сипаттары терезесі ашылады.
4. **Жалпы** бөлімінде **Push-серверді іске қосу** параметрін қосыңыз.
5. **Push-серверінің порты** өрісінде порт нөмірін көрсетіңіз. Сіз кез келген бос порттың нөмірін көрсете аласыз.
6. **Қашықтағы құрылғының мекенжайы** өрісінде тарату нүктесінің IP мекенжайын немесе атауын көрсетіңіз.
7. **OK** түймесін басыңыз.

Push сервері таңдалған тарату нүктесінде қосылған.

Клиент құрылғыларындағы үшінші тарап бағдарламалары бағдарламаларын басқару

Бұл бөлімде клиент құрылғыларындағы үшінші тарап бағдарламаларын басқарумен байланысты Kaspersky Security Center мүмкіндіктері сипатталған.

Үшінші тарап бағдарламаларының жаңартуларын орнату

Kaspersky Security Center бағдарламасы басқарылатын құрылғыларға орнатылған үшінші тарап бағдарламалық жасақтамасының жаңартуларын басқаруға, сондай-ақ қажетті жаңартуларды орнату арқылы Microsoft бағдарламалары мен басқа да бағдарламалық жасақтама өндірушілері бағдарламаларында осалдықтарды түзетуге мүмкіндік береді.

Kaspersky Security Center бағдарламасы жаңартуларды *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы көмегімен іздейді. Бұл тапсырма аяқталғаннан кейін, Басқару сервері құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап бағдарламалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады. Қолжетімді жаңартулар туралы ақпаратты көргеннен кейін, жаңартуларды құрылғыларға орнатуға болады.

Kaspersky Security Center кейбір бағдарламаларын жаңарту, бағдарламаның алдыңғы нұсқасын жою және жаңа нұсқасын орнату арқылы орындалады.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап бағдарламалық жасақтамасы жаңартулары Kaspersky технологиялары арқылы зиянды БҚ-дың бар-жоғы тұрғысынан автоматты түрде тексеріледі. Бұл технологиялар файлдарды автоматты түрде тексеру үшін қолданылады және антивирустық тексеруді, статикалық талдауды, динамикалық талдауды, "құмсалғыштың" жүріс-тұрысын талдауды және машиналық оқытуды қамтиды.

Kaspersky мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап бағдарламалық жасақтамасы жаңартуларын қолмен талдамайды. Сонымен қатар Kaspersky мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

Үшінші тарап бағдарламаларының жаңартуларын орнатуға арналған тапсырмалар

Үшінші тарап бағдарламаларын жаңарту метадеректері қоймаға жүктелген кезде, сіз келесі тапсырмаларды орындау арқылы клиент құрылғыларына жаңартуларды орната аласыз:

- *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы Windows Update жаңартулары қызметі ұсынатын жаңартуларды және басқа өндірушілердің бағдарламаларын қоса алғанда, Microsoft бағдарламаларына арналған жаңартуларды орнату үшін қолданылады. Назар аударыңыз, Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана осы тапсырманы жасауға болады.

Бұл тапсырма аяқталғаннан кейін, жаңартулар басқарылатын құрылғыларға автоматты түрде орнатылады. Жаңа жаңартулардың метадеректерін Басқару сервері қоймасына жүктеу кезінде, Kaspersky Security Center бағдарламасы жаңартулардың жаңарту ережелерінде көрсетілген критерийлерге сәйкес келетіндігін тексереді. Критерийлерге сәйкес келетін барлық жаңа жаңартулар келесі тапсырма басталған кезде автоматты түрде жүктеледі және орнатылады.

- *Windows Update жаңартуларын орнату* тапсырмасы.

  Windows Update жаңартуларын орнату тапсырмасы лицензияны қажет етпейді, бірақ оны Windows Update жаңартуларын орнату үшін ғана қолдануға болады.

  Бұл тапсырма аяқталғаннан кейін, тек тапсырманың сипаттарында көрсетілген жаңартулар орнатылады. Кейінірек, Басқару сервері қоймасына жүктелген жаңа жаңартуларды орнатқыңыз келсе, қолданыстағы тапсырманың жаңарту тізіміне қажетті жаңартуларды қосу немесе Windows Update жаңартуларын орнату тапсырмасын жасау қажет болады.

Басқару серверін WSUS сервері ретінде пайдалану

Қолжетімді Microsoft Windows жаңартулары туралы ақпарат Windows Update орталығынан беріледі. Басқару серверін Windows Update (WSUS) сервері ретінде пайдалануға болады. Басқару серверін WSUS сервері ретінде қолдану үшін, сіз Windows Update жаңартуларын синхрондау тапсырмасын жасап, **Желілік агент саясатында** Басқару серверін WSUS сервері ретінде пайдалану параметрін таңдауыңыз керек. Деректерді Windows Update орталығымен синхрондауды конфигурациялағаннан кейін, Басқару сервері құрылғылардағы Windows Update қызметтеріне жаңартуларды белгіленген жиілікпен орталықтан ұсынады.

Сценарий: Үшінші тарап бағдарламаларын жаңарту

Бұл бөлімде клиент құрылғыларында орнатылған үшінші тарап бағдарламаларын жаңарту сценарийі ұсынылған. Үшінші тарап бағдарламалары Microsoft және басқа да бағдарламалық жасақтама өндірушілері ұсынған бағдарламаларды қамтиды. Microsoft бағдарламалары үшін жаңартуларды Windows Update қызметі ұсынады.

Алдын ала талаптар

Microsoft бағдарламаларынан басқа үшінші тарап бағдарламаларының жаңартуларын орнату үшін Басқару серверінде интернет байланысы болуы керек.

Әдепкі бойынша, Басқару сервері Microsoft бағдарламасының жаңартуларын басқарылатын құрылғыларға орнату үшін интернет байланысын қажет етпейді. Мысалы, басқарылатын құрылғылар Microsoft бағдарламасының жаңартуларын тікелей Microsoft жаңарту серверлерінен немесе ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server серверінен жүктей алады. Басқару серверін WSUS сервері ретінде қолдансаңыз, Басқару сервері интернетке қосылуы керек.

Кезеңдер

Өндірушілердің жаңартуы келесі кезеңдерден тұрады:

1. **Қажетті жаңартуларды іздеу**

   Басқарылатын құрылғыларға қажет үшінші тарап бағдарламасының жаңартуларын табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосыңыз. Бұл тапсырма аяқталғаннан кейін, Kaspersky Security Center бағдарламасы құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап бағдарламалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады.

   Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы Басқару серверінің Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Егер сіз шеберді іске қоспаған болсаңыз, тапсырма жасаңыз немесе бағдарламаны жылдам іске қосу шеберін іске қосыңыз.

   Нұсқаулар:

   - Басқару консолі: Бағдарламаларда осалдықтарды іздеу, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін кестені белгілеу.
   - Kaspersky Security Center Web Console: Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы параметрлері.

2. **Табылған жаңартулар тізімін талдау**

   Бағдарламалық жасақтама жаңартулары тізімін қарап, қандай жаңартуларды орнату керектігін шешіңіз. Әрбір жаңарту туралы толық ақпаратты көру үшін тізімдегі жаңарту атын түртіңіз. Тізімдегі әрбір жаңарту үшін клиент құрылғыларындағы жаңартуларды орнату статистикасын да көруге болады.

   Нұсқаулар:

   - Басқару консолі: Қолжетімді жаңартулар туралы ақпаратты қарау.
   - Kaspersky Security Center Web Console: Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау.

3. **Жаңартулар орнатуды конфигурациялау**

   Kaspersky Security Center бағдарламасы үшінші тарап бағдарламаларының жаңартулар тізімін алғаннан кейін, сіз оларды *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын немесе *Windows Update жаңартуларын орнату* тапсырмасын қолдану арқылы клиент құрылғыларына орната аласыз. Осы тапсырмалардың бірін жасаңыз. Осы тапсырмаларды **Тапсырмалар** қойындысында немесе **Бағдарламалық жасақтама жаңартулары** тізімі көмегімен жасай аласыз.

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы Windows Update жаңартулары қызметі ұсынатын жаңартуларды және басқа өндірушілердің бағдарламаларын қоса алғанда, Microsoft бағдарламаларына арналған жаңартуларды орнату үшін қолданылады. Назар аударыңыз, Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана осы тапсырманы жасауға болады.

   Windows Update жаңартуларын орнату тапсырмасы лицензияны қажет етпейді, бірақ оны Windows Update жаңартуларын орнату үшін ғана қолдануға болады.

   Бағдарламалық жасақтаманың кейбір жаңартуларын орнату үшін сіз бағдарламалық жасақтаманы орнатуға арналған Лицензиялық келісімді қабылдауыңыз керек. Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтама жаңартулары орнатылмайды.

   Жаңартуды орнату тапсырмасын кесте бойынша іске қосуға болады. Тапсырманың кестесін көрсету кезінде, жаңартуды орнату тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама осалдықтарын түзету, Қолжетімді жаңартулар туралы ақпаратты қарау.
- Kaspersky Security Center Web Console: Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау, Windows Update жаңартуларын орнату тапсырмасын жасау, Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау.

4 **Тапсырманың кестесін белгілеу**

Жаңартулар тізімі әрқашан өзекті екеніне көз жеткізу мақсатында, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын мезгіл-мезгіл автоматты түрде іске қосылуы үшін, оны іске қосу кестесін белгілеңіз. Әдепкі бойынша *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы сағат 18:00:00-де қолмен іске қосылады.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, сіз оны *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосумен бірдей немесе одан сирек жиілікпен іске қосуды белгілей аласыз. *Windows Update жаңартуларын орнату* тапсырмасын жоспарлау кезінде, бұл тапсырма үшін, осы тапсырманы іске қосудың алдында әрбір рет жаңартулар тізімін анықтауыңыз керек екеніне назар аударыңыз.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5 **Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау (қажет болса)**

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, сіз тапсырманың сипаттарында жаңартуларды орнату ережелерін көрсете аласыз. Windows Update жаңартуларын орнату тапсырмасын жасаған болсаңыз, бұл қадамды өткізіп жіберіңіз.

Әрбір ереже үшін, жаңарту күйіне байланысты орнату үшін жаңартуларды анықтай аласыз: *Анықталмаған*, *Расталды* немесе *Қабылданбады*. Мысалы, сіз серверлер үшін белгілі бір тапсырма жасай аласыз және тек Windows Update жаңартуларын ғана және тек *Расталды* күйі бар жаңартуларды ғана орнатуға рұқсат беру үшін осы тапсырмаға арналған ережені орната аласыз. Содан кейін, орнатқыңыз келетін жаңартулар үшін *Расталды* күйін қолмен белгілейсіз. Бұл жағдайда, *Анықталмаған* немесе *Қабылданбады* күйі бар Windows Update жаңартулары тапсырмада көрсетілген серверлерге орнатылмайды.

Жаңартуларды орнатуды басқарған кезде, аздаған жаңартулар үшін *Расталды* күйін қолданған жөн. Бірнеше жаңарту орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасында конфигурациялауға болатын ережелерді қолданыңыз. *Расталды* күйін, ережелерде көрсетілген өлшемшарттарға сай келмейтін жаңартулар үшін ғана белгілеу ұсынылады. Жаңартулардың көп санын қолмен растау кезінде, Басқару серверінің өнімділігі төмендеп, бұл Басқару серверінің артық жүктелуіне әкелуі мүмкін.

Әдепкі бойынша, жүктелген бағдарламалық жасақтама жаңартулары *Анықталмаған* күйіне ие. Күйді **Бағдарламалық жасақтама жаңартулары** (**Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары**) тізімінде *Расталды* немесе *Қабылданбады* деп өзгерте аласыз.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама жаңартуын мақұлдау және қабылдамау
- Kaspersky Security Center Web Console: Үшінші тарап бағдарламалары жаңартуларын растау және қабылдамау

6 **Басқару серверін Windows Server Жаңарту қызметтері (WSUS) ретінде жұмыс істеу үшін конфигурациялау (қажет болса)**

Әдепкі бойынша, Windows Update жаңартулары Microsoft серверлерінен басқарылатын құрылғыларға жүктеледі. Басқару серверін WSUS сервері ретінде пайдалану үшін осы параметрді өзгерте аласыз. Бұл жағдайда, Басқару сервері жаңарту деректерін белгіленген жиілікпен Windows Update қызметімен синхрондайды және жаңартуларды желілік құрылғылардағы Windows Update қызметтеріне орталықтандырылған түрде ұсынады.

Басқару серверін WSUS сервері ретінде қолдану үшін, сіз Windows Update жаңартуларын синхрондау тапсырмасын жасап, Желілік агент саясатында **Басқару серверін WSUS сервері ретінде пайдалану** жалаушасын қойыңыз.

Нұсқаулар:

- Басқару консолі: Windows Update жаңартуларын Басқару серверімен синхрондау, Желілік агент саясатында Windows жаңартуларын конфигурациялау
- Kaspersky Security Center Web Console: Windows Update жаңартуларын синхрондау тапсырмасын жасау

7. **Жаңартуларды орнату тапсырмасын іске қосу**

   Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын немесе *Windows Update жаңартуларын орнату* тапсырмасын іске қосыңыз. Осы тапсырмаларды орындағаннан кейін, жаңартулар жүктеледі және басқарылатын құрылғыларға орнатылады. Тапсырма аяқталғаннан кейін, оның тапсырмалар тізімінде *Сәтті аяқталды* күйі бар екеніне көз жеткізіңіз.

8. **Үшінші тарап бағдарламаларының жаңартуларын орнату нәтижелері туралы есепті құрастыру (қажет болса)**

   Жаңартуды орнату статистикасын қарау үшін, **Үшінші тарап бағдарламалық жасақтамасы жаңартуларын орнату нәтижелерін хабарлау** құрастырыңыз.

   Нұсқаулар:

   - Басқару консолі: Есепті жасау және қарау
   - Kaspersky Security Center Web Console: Есепті жасау және қарау

Нәтижелер

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған және конфигурациялаған болсаңыз, жаңартулар басқарылатын құрылғыларға автоматты түрде орындалатын болады. Жаңа жаңартуларды Басқару сервері қоймасына жүктеу кезінде, Kaspersky Security Center бағдарламасы жаңартулардың жаңарту ережелерінде көрсетілген критерийлерге сәйкес келетіндігін тексереді. Критерийлерге сәйкес келетін барлық жаңа жаңартулар келесі тапсырма басталған кезде автоматты түрде орнатылады.

Windows Update жаңартуларын орнату тапсырмасын жасаған болсаңыз, *Windows Update жаңартуларын орнату* тапсырмасының сипаттарында көрсетілетін жаңартулар ғана орнатылады. Кейінірек, Басқару сервері қоймасына жүктелген жаңа жаңартуларды орнатқыңыз келсе, қолданыстағы тапсырманың жаңарту тізіміне қажетті жаңартуларды қосу немесе *Windows Update жаңартуларын орнату* тапсырмасын жасау қажет болады.

Үшінші тарап бағдарламаларының жаңартуларын орнату

Келесі тапсырмалардың бірін жасау және іске қосу арқылы басқарылатын құрылғыларға үшінші тарап бағдарламалық жасақтамасының жаңартуларын орнатуға болады:

- *Қажетті жаңартуларды орнату және осалдықтарды түзету*

  Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын, тек Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана жасауға болады. Бұл тапсырманы Microsoft ұсынған Windows Update жаңартуларын және басқа өндірушілер ұсынған бағдарламалардың жаңартуларын орнату үшін пайдалануға болады.

- *Windows Update жаңартуларын орнату*

  Windows Update жаңартуларын орнату тапсырмасын тек Windows Update жаңартуларын орнату үшін ғана қолдануға болады.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Сондай-ақ, қажетті жаңартуларды келесі жолдармен орнату үшін тапсырма жасауға болады:

- Жаңартулар тізімін ашып, қандай жаңартуларды орнату керектігін көрсетіңіз.

  Нәтижесінде, таңдалған жаңартуларды орнату үшін тапсырма жасалады. Сондай-ақ, таңдалған жаңартуларды қолданыстағы тапсырмаға қосуға болады.

- Жаңартуды орнату шеберін іске қосу.

  Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері қолжетімді болады.

  Шебер жаңартуларды орнату тапсырмасын құруды және конфигурациялауды жеңілдетеді және орнату үшін бірдей жаңартуларды қамтитын артық тапсырмаларды құруды болдырмайды.

Жаңарту тізімін пайдаланып, үшінші тарап бағдарламаларының жаңартуларын орнату

Үшінші тарап бағдарламаларының жаңартуларын орнату үшін:

1. Жаңарту тізімдерінің бірін ашыңыз:

   - Жалпы жаңартулар тізімін ашу үшін, **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.
   - Басқарылатын құрылғы үшін жаңартулар тізімін ашу үшін **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** → <құрылғы атауы> → **Кеңейтілген** → **Қолжетімді жаңартулар** бөліміне өтіңіз.
   - Белгіленген бағдарламаның жаңартулар тізімін ашу үшін **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** → <бағдарлама атауы> → **Қолжетімді жаңартулар** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Орнатқыңыз келетін жаңартулардың жанына жалаушаны қойыңыз.

3. **Жаңартуларды орнату** түймесін басыңыз.

   Бағдарламалық жасақтаманың кейбір жаңартуларын орнату үшін сіз Лицензиялық келісімді қабылдауыңыз керек. Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтама жаңартулары орнатылмайды.

4. Келесі нұсқалардың бірін таңдаңыз:

   - **Жаңа тапсырма**

     Жаңа тапсырма жасау шебері іске қосылады. Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, әдепкі бойынша *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырма түрі таңдалады. Лицензияңыз болмаса, әдепкі бойынша *Windows Update жаңартуларын орнату* тапсырма түрі таңдалады. Тапсырма жасауды аяқтау үшін шебердің алдағы нұсқауларын орындаңыз.

   - **Жаңартуды орнату (көрсетілген тапсырмаға ереже қосу)**

     Таңдалған жаңартуларды қосқыңыз келетін тапсырманы таңдаңыз. Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын таңдаңыз. Таңдалған жаңартуларды орнату үшін жаңа ереже автоматты түрде таңдалған тапсырмаға қосылатын болады. Лицензияңыз болмаса, әдепкі бойынша *Windows Update жаңартуларын орнату* тапсырма түрі таңдалады. Таңдалған жаңартулар тапсырманың сипаттарына қосылды.

     Тапсырма сипаттары терезесі ашылады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

   Тапсырма жасауды таңдаған болсаңыз, ол тапсырмалар тізімінде, **Активтер (құрылғылар)** → **Тапсырмалар** бөлімінде жасалып, көрсетіледі Егер сіз бар тапсырмаға жаңартуларды қосуды таңдасаңыз, жаңартулар тапсырма сипаттарында сақталады.

Үшінші тарап бағдарламаларын орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын немесе *Windows Update жаңартуларын орнату* тапсырмасын іске қосыңыз. Осы тапсырмаларды қолмен іске қоса аласыз немесе іске қосып жатқан тапсырманың сипаттарында кестені белгілей аласыз. Тапсырманың кестесін көрсету кезінде, жаңартуды орнату тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

Жаңартуды орнату шебері арқылы үшінші тарап бағдарламаларының жаңартуларын орнату

Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, жаңартуды орнату шебері қолжетімді болады.

Жаңартуды орнату шеберін пайдаланып, үшінші тарап бағдарламалары жаңартуларын орнату тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Орнатқыңыз келетін жаңартудың жанына жалаушаны қойыңыз.

3. **Жаңартуларды орнату шеберін іске қосу** түймесін басыңыз.

   Жаңартуды орнату шеберін іске қосылады. **Жаңа нұсқаны орнату тапсырмасын таңдау** бетінде келесі түрдегі барлық қолданыстағы тапсырмалар тізімі көрсетіледі:

   - *Қажетті жаңартуларды орнату және осалдықтарды түзету*
   - *Windows Update жаңартуларын орнату*
   - *Осалдықтарды түзету*

   Жаңа жаңартуларды орнату үшін соңғы екі түрдегі тапсырмаларды өзгерту мүмкін емес. Жаңа жаңартуларды орнату үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын ғана қолдануға болады.

4. Егер сіз шебердің сіз таңдаған жаңартуды орнататын тапсырмаларды ғана көрсетуін қаласаңыз, **Осы жаңа нұсқаны орнататын тапсырмаларды ғана көрсету** параметрін қосыңыз.

5. Орындағыңыз келетін әрекетті таңдаңыз:

   - Тапсырманы іске қосу үшін, тапсырманың аты жанында жалаушаны қойып, **Іске қосу** түймесін басыңыз.
   - Қолданыстағы тапсырмаға жаңа ережені қосу үшін:

     a. Тапсырманың аты жанына жалаушаны қойып, **Ереже қосу** түймесін басыңыз.

     b. Ашылған бетте жаңа ережені орнатыңыз:

     - **Осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

       Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

       Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

Әдепкі бойынша, параметр өшірулі.

- **MSRC бойынша осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

  Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

  Егер бұл параметр қосылса (Windows Update жаңартулары үшін ғана қолжетімді), жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

  Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

  Әдепкі бойынша, параметр өшірулі.

- **Осы жеткізушінің жаңартуларын орнату ережесі**

  Бұл параметр тек үшінші тарап бағдарламаларын жаңарту үшін қолжетімді. Kaspersky Security Center тек таңдалған жаңартумен бірдей өндірушінің бағдарламаларына қатысты жаңартуларды орнатады. Басқа өндірушілердің қабылданбаған жаңартулары мен бағдарлама жаңартулары орнатылмайды.

  Әдепкі бойынша, параметр өшірулі.

- **түрінің жаңартулары үшін орнату ережесі**

- **Таңдалған жаңартуды орнату ережесі**

- **Таңдалған жаңартуларды мақұлдау**

  Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

- **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

  Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

  Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

  Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

  Әдепкі бойынша, параметр қосулы.

c. **Қосу** түймесін басыңыз.

- Тапсырма жасау үшін:

  a. **Жаңа тапсырма** түймесін басыңыз.

  b. Ашылған бетте жаңа ережені орнатыңыз:

  - **Осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

    Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

    Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

    Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

    Әдепкі бойынша, параметр өшірулі.

  - **MSRC бойынша осы маңыздылық деңгейінің жаңартулары үшін орнату ережесі**

    Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

    Егер бұл параметр қосылса (Windows Update жаңартулары үшін ғана қолжетімді), жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

    Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

    Әдепкі бойынша, параметр өшірулі.

  - **Осы жеткізушінің жаңартуларын орнату ережесі**

    Бұл параметр тек үшінші тарап бағдарламаларын жаңарту үшін қолжетімді. Kaspersky Security Center тек таңдалған жаңартумен бірдей өндірушінің бағдарламаларына қатысты жаңартуларды орнатады. Басқа өндірушілердің қабылданбаған жаңартулары мен бағдарлама жаңартулары орнатылмайды.

    Әдепкі бойынша, параметр өшірулі.

  - **түрінің жаңартулары үшін орнату ережесі**

  - **Таңдалған жаңартуды орнату ережесі**

  - **Таңдалған жаңартуларды мақұлдау**

    Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

    Әдепкі бойынша, параметр өшірулі.

  - **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

Әдепкі бойынша, параметр қосулы.

c. **Қосу** түймесін басыңыз.

Егер сіз тапсырманы іске қосуды шешсеңіз, шеберді жабуға болады. Тапсырма фондық режимде орындалады. Қосымша әрекеттер қажет емес.

Егер сіз бар тапсырмаға ереже қосуды таңдасаңыз, тапсырма сипаттары терезесі ашылады. Тапсырманың сипаттарына жаңа ереже қосылды. Ережені, сондай-ақ басқа тапсырма параметрлерін көруге немесе өзгертуге болады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Тапсырма жасауды шешсеңіз, оны тапсырма жасау шеберінің көмегімен жасаңыз. Жаңартуды орнату шеберінде қосқан жаңа ереже тапсырма жасау шеберінде көрсетіледі. Шебердің жұмысы аяқталғаннан кейін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы тапсырмалар тізіміне қосылады.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасының көмегімен Kaspersky Security Center бағдарламасы басқарылатын құрылғыларға орнатылған үшінші тарап бағдарламалары үшін табылған осалдықтар мен қажетті жаңартулар тізімдерін алады.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бағдарламаны жылдам іске қосу шебері жұмыс істеп тұрған кезде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы қолмен жасай аласыз.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Security Center бағдарламасы үшін **Осалдықтарды және қажетті жаңартуларды іздеу** тапсырма түрін таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

6. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

7. **Жасау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

8. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

9. Тапсырма сипаттары терезесінде тапсырманың жалпы параметрлерін көрсетіңіз.

10. **Бағдарлама параметрлері** қойындасында келесі параметрлерді көрсетіңіз:

    - **Microsoft тізіміндегі осалдықтар мен жаңартуларды іздеңіз**

      Осалдықтар мен жаңартуларды іздеу кезінде Kaspersky Security Center бағдарламасы ағымдағы сәтте қолжетімді Microsoft жаңартулардың көздерінен Microsoft қолжетімді жаңартулары туралы деректерді қолданады.

      Мысалы, Microsoft жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

      Әдепкі бойынша, параметр қосулы.

      Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

    - **Деректерді жаңарту үшін жаңарту серверіне қосылу**

      Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

      - Kaspersky Security Center Басқару сервері (Желілік агент саясатының параметрлерін қараңыз).
      - Ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server.
      - Microsoft жаңарту серверлері.

      Егер бұл параметр қосулы болса, басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылып, Microsoft Windows қолжетімді жаңартулары туралы ақпарат алады.

      Егер бұл параметр өшірулі болса, басқарылатын құрылғыдағы Windows Update агенті бұған дейін Microsoft жаңарту көзінен алған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты пайдаланады.

      Microsoft жаңарту көзіне қосылу ресурстарды қажет етуі мүмкін. Егер сіз осы жаңарту көзіне басқа тапсырмада немесе Желілік агент саясатының сипаттарында, **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** бөлімінде тұрақты қосылым орнатқан болсаңыз, бұл параметрді өшіре аласыз Егер сіз бұл параметрді өшіргіңіз келмесе, Серверге түсетін жүктемені азайту үшін тапсырмалар кестесін 360 минут аралығындағы тапсырманы іске қосу кідірісінің кездейсоқ мәнін пайдалануға болатындай конфигурациялауға болады.

      Әдепкі бойынша, параметр қосулы.

Желілік агент саясаты параметрлерінің келесі мәндерінің тіркесімі жаңартуларды алу режимін анықтайды:

- Басқарылатын құрылғыдағы Windows Update агенті жаңартуларды алу үшін жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының сипаттарында қосылған және **Windows Update жаңартуларын іздеу режимі** параметрі желілік агент саясатының параметрлерінде **Белсенді** болып белгіленген жағдайда ғана қосылады.

- *Осалдықты сканерлеу* тапсырмасын орындаған кезде Microsoft Windows жаңарту көзіне қосылымды бастау және жаңартуларды жүктеп алу үшін Желілік агент қажет болмаса, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатуға болады, бұл арада **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы күйде қала беруі керек. Бұл, ресурстарды үнемдеуге және осалдықтарды іздеу үшін бұрын алынған Windows жаңартуларын пайдалануға мүмкіндік береді. Microsoft Windows жаңартуларын алуды басқа тәсілмен конфигурациялаған болсаңыз, пассивті режимді пайдалануға болады. Microsoft Windows жаңартуларын басқа жолмен алу үшін конфигурацияланбасаңыз, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатпаңыз, себебі бұл жағдайда жаңартулар туралы ақпарат ешқашан алынбайды.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметріне қарамастан (қосулы немесе өшірулі), егер **Windows Update жаңартуларын іздеу режимі** параметрі үшін **Өшірулі** параметрлер тобында таңдалса, онда Kaspersky Security Center бағдарламасы жаңартулар туралы ақпаратты сұрамайды.

- **Kaspersky ұсынған үшінші тарап осалдықтары мен жаңартуларын іздеңіз**

  Егер бұл параметр қосулы болса, Kaspersky Security Center бағдарламасы Windows тізімдемесінде және **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз** бөлімінде көрсетілген қалталарда үшінші тарап өндірушілерінің бағдарламалары (Kaspersky және Microsoft-тан басқа өндірушілер шығарған бағдарламалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап бағдарламаларының толық тізімін Kaspersky бақылайды.

  Егер бұл параметр өшірулі болса, Kaspersky Security Center бағдарламасы үшінші тарап бағдарламалары үшін осалдықтар мен қажетті жаңартуларды іздемейді. Мысалы, Microsoft Windows жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

- **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсету**

  Kaspersky Security Center бағдарламасы осалдықтарды түзетуді және жаңартуларды орнатуды қажет ететін үшінші тарап бағдарламаларын іздейтін қалталар. Жүйе айнымалыларын пайдалануға болады.

  Бағдарламалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген бағдарламалар орнатылған жүйелік қалталар бар.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

11. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Тапсырманың нәтижелерінде 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" қатесі туралы ескерту бар болса, бұл мәселені Windows тізімдемесі арқылы шешуге болады.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы параметрлері

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы бағдарламаны жылдам іске қосу шебері жұмыс істеп тұрған кезде автоматты түрде жасалады. Қолданбаның жылдам іске қосу шеберін іске қоспаған болсаңыз, тапсырманы қолмен жасай аласыз.

Тапсырманың жалпы параметрлерінен бөлек, *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын жасау кезінде немесе кейінірек, жасалған тапсырманың сипаттарын конфигурациялау кезінде келесі параметрлерді көрсете аласыз:

- **Microsoft тізіміндегі осалдықтар мен жаңартуларды іздеңіз**

  Осалдықтар мен жаңартуларды іздеу кезінде Kaspersky Security Center бағдарламасы ағымдағы сәтте қолжетімді Microsoft жаңартулардың көздерінен Microsoft қолжетімді жаңартулары туралы деректерді қолданады.

  Мысалы, Microsoft жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

  Әдепкі бойынша, параметр қосулы.

  Қосымша Microsoft Windows жаңартулары туралы ақпарат басқару серверіне жіберілмейді.

- **Деректерді жаңарту үшін жаңарту серверіне қосылу**

  Басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылады. Келесі қызметтер Microsoft жаңарту көздері бола алады:

  - Kaspersky Security Center Басқару сервері (Желілік агент саясатының параметрлерін қараңыз).
  - Ұйымыңыздың желісінде орналастырылған Microsoft Windows Server Update Services (WSUS) қызметтері бар Windows Server.
  - Microsoft жаңарту серверлері.

  Егер бұл параметр қосулы болса, басқарылатын құрылғыдағы Windows Update агенті Microsoft жаңарту көзіне қосылып, Microsoft Windows қолжетімді жаңартулары туралы ақпарат алады.

  Егер бұл параметр өшірулі болса, басқарылатын құрылғыдағы Windows Update агенті бұған дейін Microsoft жаңарту көзінен алған Microsoft Windows қолжетімді жаңартулары туралы ақпаратты пайдаланады.

  Microsoft жаңарту көзіне қосылу ресурстарды қажет етуі мүмкін. Егер сіз осы жаңарту көзіне басқа тапсырмада немесе Желілік агент саясатының сипаттарында, **Бағдарламалық жасақтаманың жаңартулары мен осалдықтары** бөлімінде тұрақты қосылым орнатқан болсаңыз, бұл параметрді өшіре аласыз Егер сіз бұл параметрді өшіргіңіз келмесе, Серверге түсетін жүктемені азайту үшін тапсырмалар кестесін 360 минут аралығындағы тапсырманы іске қосу кідірісінің кездейсоқ мәнін пайдалануға болатындай конфигурациялауға болады.

  Әдепкі бойынша, параметр қосулы.

  Желілік агент саясаты параметрлерінің келесі мәндерінің тіркесімі жаңартуларды алу режимін анықтайды:

  - Басқарылатын құрылғыдағы Windows Update агенті жаңартуларды алу үшін жаңарту серверіне тек **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының сипаттарында қосылған және **Windows Update жаңартуларын іздеу режимі** параметрі желілік агент саясатының параметрлерінде **Белсенді** болып белгіленген жағдайда ғана қосылады.
  - *Осалдықты сканерлеу* тапсырмасын орындаған кезде Microsoft Windows жаңарту көзіне қосылымды бастау және жаңартуларды жүктеп алу үшін Желілік агент қажет болмаса, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатуға болады, бұл арада **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметрі қосулы күйде қала беруі керек. Бұл, ресурстарды үнемдеуге және осалдықтарды іздеу үшін бұрын алынған Windows жаңартуларын пайдалануға мүмкіндік береді. Microsoft Windows жаңартуларын алуды басқа тәсілмен конфигурациялаған болсаңыз, пассивті режимді пайдалануға болады. Microsoft Windows жаңартуларын басқа жолмен алу үшін конфигурацияланбасаңыз, **Windows Update жаңартуларын іздеу режимі** параметрін **Пассив** күйіне орнатпаңыз, себебі бұл жағдайда жаңартулар туралы ақпарат ешқашан алынбайды.
  - **Деректерді жаңарту үшін жаңарту серверіне қосылу** параметріне қарамастан (қосулы немесе өшірулі), егер **Windows Update жаңартуларын іздеу режимі** параметрі үшін **Өшірулі** параметрлер тобында таңдалса, онда Kaspersky Security Center бағдарламасы жаңартулар туралы ақпаратты сұрамайды.

- **Kaspersky ұсынған үшінші тарап осалдықтары мен жаңартуларын іздеңіз**

  Егер бұл параметр қосулы болса, Kaspersky Security Center бағдарламасы Windows тізімдемесінде және **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсетіңіз** бөлімінде көрсетілген қалталарда үшінші тарап өндірушілерінің бағдарламалары (Kaspersky және Microsoft-тан басқа өндірушілер шығарған бағдарламалар) үшін осалдықтар мен қажетті жаңартуларды іздейді. Қолдау көрсетілетін үшінші тарап бағдарламаларының толық тізімін Kaspersky бақылайды.

Егер бұл параметр өшірулі болса, Kaspersky Security Center бағдарламасы үшінші тарап бағдарламалары үшін осалдықтар мен қажетті жаңартуларды іздемейді. Мысалы, Microsoft Windows жаңартулары мен өзге өнімдердің жаңартулары үшін әртүрлі параметрлері бар әртүрлі тапсырмалар болса, осы параметрді өшіруге болады.

Әдепкі бойынша, параметр қосулы.

- **Файлдық жүйеде бағдарламаларды қосымша іздеу жолдарын көрсету**

  Kaspersky Security Center бағдарламасы осалдықтарды түзетуді және жаңартуларды орнатуды қажет ететін үшінші тарап бағдарламаларын іздейтін қалталар. Жүйе айнымалыларын пайдалануға болады.

  Бағдарламалар орнатылған қалталарды көрсетіңіз. Әдепкі бойынша, тізімде көптеген бағдарламалар орнатылған жүйелік қалталар бар.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

Тапсырма кестесін конфигурациялау бойынша ұсыныстар

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын іске қосу кестесін жоспарлау кезінде, **Өткізіп алынған тапсырмаларды іске қосу** және **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** параметрлерінің қосулы екеніне көз жеткізіңіз.

Әдепкі бойынша *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы сағат 18:00:00-де қолмен іске қосылады. Егер ұйымның жұмыс регламенті осы уақытта құрылғыларды өшіруді көздесе, онда *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыны қосқаннан кейін (келесі күні таңертең) іске қосылады. Мұнда жүріс-тұрыс жағымсыз болуы мүмкін, өйткені осалдықтарды іздеу құрылғының процессоры мен диск ішкі жүйесіне жоғары жүктеме түсіруі мүмкін. Ұйымда қабылданған жұмыс регламентіне сүйене отырып, тапсырманың оңтайлы кестесін конфигурациялау керек.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, Осалдықтар мен патчтарды басқару лицензия болған кезде қолжетімді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, үшінші тарап бағдарламаларында, соның ішінде басқарылатын құрылғыларға орнатылған Microsoft бағдарламаларында жаңарту және осалдықтарды түзету үшін қолданылады. Бұл тапсырма бірнеше жаңартуларды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықтарды түзетуге мүмкіндік береді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасының көмегімен жаңартуларды орнату немесе осалдықтарды түзету үшін, сіз келесі әрекеттердің бірін орындай аласыз:

- Жаңартуды орнату шеберін немесе осалдықтарды түзету шеберін іске қосыңыз.
- *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасаңыз.
- Қолданыстағы *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасына жаңартуды орнату ережесін қосыңыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.
3. Kaspersky Security Center бағдарламасы үшін **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырма түрін таңдаңыз.

   Тапсырма көрсетілмесе, есептік жазбада **Жүйені басқару**: **Осалдықтар мен патчтарды басқару** функционалды аймағына арналған **Оқу**, **өзгерту** және **орындау** құқықтары бар екенін тексеріңіз. Сіз осы қатынас құқықтарынсыз *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасай алмайсыз және конфигурациялай алмайсыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.
6. Жаңартуларды орнату ережелерін, содан соң келесі параметрлерді көрсетіңіз:

   - **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау**

     Егер жалауша қойылса, құрылғыны қайта іске қоспас немесе өшірмес бұрын жаңартуды орнату орындалады. Әйтпесе, жаңартуларды орнату кесте бойынша жүзеге асырылады.

     Жаңартуларды орнату құрылғылардың жұмысына әсер етуі мүмкін болса, осы жалаушаны қойыңыз.

     Әдепкі бойынша, параметр өшірулі.

- **Қажетті жалпы жүйелік құрамдастарды орнату**

  Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

  Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартулар кезінде бағдарламаның жаңа нұсқаларын орнатуға рұқсат ету**

  Бұл опция қосылған болса, бағдарламалық жасақтама қолданбасының жаңа нұсқасын орнатуға әкелсе, жаңартуларға рұқсат беріледі.

  Бұл параметр өшірулі болса, бағдарлама жаңартылмайды. Бағдарламалардың жаңа нұсқаларын кейінірек қолмен немесе басқа тапсырманы қолдана отырып, орнатуға болады. Мысалы, егер сіздің компанияңыздың инфрақұрылымы бағдарламаның жаңа нұсқасын қолдамаса немесе сынақ инфрақұрылымындағы жаңартуды тексеру қажет болса, бұл параметрді пайдалануға болады.

  Әдепкі бойынша, параметр қосулы.

  > Бағдарламаның жаңа нұсқасын орнатқаннан кейін, клиент құрылғыларында орнатылған және жаңартылатын бағдарламаның жұмысына байланысты басқа бағдарламалардың жұмысы бұзылуы мүмкін.

- **Жаңартуларды құрылғыға орнатпастан жүктеп алу**

  Егер жалауша қойылса, бағдарлама жаңартуларды құрылғыға жүктейді, бірақ оларды автоматты түрде орнатпайды. Содан кейін, жүктелген жаңартуларды қолмен орнатуға болады.

  Microsoft жаңартулары Windows қызметтік қалтасына жүктеледі. Үшінші тарап бағдарламаларының жаңартулары (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) **Жаңартуларды келесі жерге жүктеп алу** өрісінде көрсетілген қалтаға жүктеледі.

  Егер бұл параметр өшірулі болса, жаңартулар құрылғыға автоматты түрде орнатылады.

  Әдепкі бойынша, параметр өшірулі.

- **Жаңартуларды келесі жерге жүктеп алу**

  Бұл қалта, үшінші тарап бағдарламаларының (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) жаңартуларын жүктеу үшін қолданылады.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

7. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сұрауды қайталау жиілігі (мин)**

  Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

- **Келесі уақыттан кейін қайта іске қосу (мин)**

  Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сессияларда бағдар. келесі уақыттан кейін мәжбүрлеп жабу (мин)**

  Пайдаланушының құрылғысы бұғатталған кезде бағдарламаларды мәжбүрлеп аяқтау (белсенді емес кезеңнен кейін автоматты түрде немесе қолмен).

  Егер параметр қосулы болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы енгізу өрісінде көрсетілген уақыт өткеннен кейін тоқтатылады.

  Егер параметр өшірулі болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы тоқтамайды.

  Әдепкі бойынша, параметр өшірулі.

8. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

9. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

10. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

11. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіңіз.

12. **Сақтау** түймесін басыңыз.

    Тапсырма жасалды және конфигурацияланды.

Тапсырманың нәтижелерінде 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" қатесі туралы ескерту бар болса, бұл мәселені Windows тізімдемесі арқылы шешуге болады.

Жаңартуларды орнату үшін ережелер қосу

Бұл функционалдық, Осалдықтар мен патчтарды басқаруға арналған лицензия болған кезде қолжетімді.

Бағдарламалық жасақтама жаңартуларын орнату немесе *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын қолдана отырып, бағдарламалардағы осалдықтарды түзету кезінде жаңартуларды орнату ережелерін көрсету қажет. Бұл ережелер орнатылатын жаңартуларды және түзетілетін осалдықтарды анықтайды.

Нақты параметрлер барлық Windows Update жаңартулары үшін немесе үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін ереже қосатыныңызға байланысты (яғни Kaspersky немесе Microsoft шығармаған бағдарламалар). Windows Update жаңартулары немесе үшінші тарап бағдарламаларының жаңартулары үшін ереже қосқанда, жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдауға болады. Барлық жаңартулар үшін ереже қосқанда, сіз орнатылатын жаңартуларды және жаңартуларды орнату арқылы түзетілетін осалдықтарды таңдай аласыз.

Жаңартуларды орнату ережесін келесі жолдармен қосуға болады:

- Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау кезінде ереже қосу.
- **Бағдарлама параметрлері** қойыншасында, тиісті *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы сипаттары терезесінде ереже қосу.
- Жаңартуды орнату шебері немесе осалдықтарды түзету шебері көмегімен.

Барлық жаңартуларге ережені қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрі** бетінде **Барлық жаңартуларға арналған ереже** тармағын таңдаңыз.

3. Ашылмалы тізімдегі **Жалпы критерийлер** терезесінде келесі параметрлерді көрсетіңіз:

- **Орнатылатын жаңартулар жиынтығы**

  Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

  - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
  - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
  - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

- **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

  Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

  Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

  Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

  Әдепкі бойынша, параметр өшірулі.

4. **Жаңартулар** терезесінде орнатылатын жаңартуларды таңдаңыз:

- **Барлық жарамды жаңартуларды орнату**

  Бұл жағдайда, **Жалпы критерийлер** шебері терезесінде көрсетілген өлшемшарттарға сәйкес келетін бағдарламалық жасақтаманың барлық жаңартулары орнатылады. Әдепкі бойынша таңдалған.

- **Тек тізімдегі жаңартуларды орнату**

  Бұл жағдайда, тізімде қолмен таңдайтын бағдарламалық жасақтаманың жаңартулары ғана орнатылады. Бұл тізімде барлық қолжетімді бағдарламалық жасақтама жаңартулары бар.

  Мысалы, келесі жағдайларда жаңартуларды орнатуға болады: тек критикалық маңызды бағдарламаларды жаңарту үшін немесе тек қажетті бағдарламаларды жаңарту үшін сынақ ортасында жаңартуларды орнатуды тексеру.

  - **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

    Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

    Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

    Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

Әдепкі бойынша, параметр қосулы.

5. **Осалдықтар** терезесінде, көрсетілген жаңартуды орнатумен түзетілетін осалдықтарды таңдаңыз:

   - **Қалған критерийлерге сай барлық осалдықтарды жабу**

     Бұл жағдайда, **Жалпы критерийлер** шебері терезесінде көрсетілген өлшемшарттарға сәйкес келетін бағдарламалық жасақтаманың барлық осалдықтары түзетіледі. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі осалдықтарды жабу**

     Тізімнен қолмен таңдалған осалдықтарды ғана түзетіңіз. Бұл тізімде барлық анықталған осалдықтар бар.

     Мысалы, келесі жағдайларда осалдықтарды белгілеуге болады: сынақ ортасындағы осалдықтардың түзетілуін тексеру, тек маңызды бағдарламалардағы осалдықтарды түзету немесе тек қажетті бағдарламалардағы осалдықтарды түзету үшін.

6. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Windows Update жаңартуларына ережені қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрі** бетінде **Windows Update жаңартуларына арналған ереже** тармағын таңдаңыз.

3. **Жалпы шарттар** терезесінде келесі параметрлерді конфигурациялаңыз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

- **MSRC бойынша қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

  Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

  Егер бұл параметр қосылса, жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

  Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

  Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Жаңартулардың санаттары** терезесінде орнату үшін жаңарту санаттарын таңдаңыз. Бұл санаттар Microsoft Update каталогымен бірдей. Әдепкі бойынша барлық санаттар таңдалған.

6. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Үшінші тарап бағдарламаларын жаңарту ережесін қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрі** бетінде **Үшінші тарап жаңартуларға арналған ереже** тармағын таңдаңыз.

3. **Жалпы шарттар** терезесінде келесі параметрлерді конфигурациялаңыз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.

     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.

     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, Параметрлер бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Windows Update жаңартуларын орнату тапсырмасын жасау

Windows Update жаңартуларын орнату тапсырмасы Windows Update қызметі ұсынатын бағдарламалық жасақтама жаңартуларын басқарылатын құрылғыларға орнатуға мүмкіндік береді.

Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болмаса, сіз *Windows Update жаңартуларын орнату* түріндегі тапсырмаларды жасай аласыз. Жаңа жаңартуларды орнату үшін, оларды қолданыстағы *Windows Update жаңартуларын орнату* тапсырмасына қоса аласыз. *Windows Update жаңартуларын орнату* тапсырмасы орнына *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын қолдану ұсынылады. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы автоматты түрде бірнеше жаңартуды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықты түзетуге мүмкіндік береді. Сондай-ақ, бұл тапсырма үшінші тарап бағдарламалары, яғни Microsoft емес өндіріс бағдарламалары үшін жаңартуларды орнатуға мүмкіндік береді.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Windows Update жаңартуларын орнату тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. Kaspersky Security Center бағдарламасы үшін **Windows Update жаңартуларын орнату** тапсырма түрін таңдаңыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

6. **Қосу** түймесін басыңыз.

   Жаңартулар тізімі ашылады.

7. Орнатқыңыз келетін Windows Update жаңартуларын таңдаңыз және **OK** түймесін басыңыз.

8. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сұрауды қайталау жиілігі (мин)**

  Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

- **Келесі уақыттан кейін қайта іске қосу (мин)**

  Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

9. Есептік жазба параметрлерін белгілеңіз:

   - **Әдепкі есептік жазба**

     Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Есептік жазбаны көрсету**

     Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

   - **Есептік жазба**

     Тапсырманы іске қосатын есептік жазба.

   - **Құпиясөз**

     Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

10. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

11. **Аяқтау** түймесін басыңыз.

    Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

12. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

13. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіңіз.

14. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Үшінші тарап бағдарламаларының қолжетімді жаңартулары туралы ақпаратты қарау

Клиент құрылғыларында орнатылған Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін көруге болады.

Клиент құрылғыларында орнатылған үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

Қолжетімді жаңартулар тізімі көрсетіледі.

Бағдарлама жаңартулары тізімін қарау үшін сүзгіні көрсете аласыз. Сүзгіні басқару бағдарламаларын жаңарту тізімінің жоғарғы оң жақ бұрышындағы **Сүзгі** ( ) белгішесін түртіңіз. Сонымен қатар, бағдарламалық жасақтама осалдықтары тізімінің үстіндегі **Алдын ала орнатылған сүзгілер** ашылмалы тізімінде алдын ала орнатылған сүзгілердің бірін таңдай аласыз.

Жаңарту сипаттарын көру үшін:

1. Қажетті бағдарламалық жасақтама жаңартуының атын түртіңіз.
2. Қойындылар бойынша топтастырылған келесі ақпаратты көрсететін жаңарту сипаттары терезесі ашылады:

   - **Жалпы**

     Бұл қойынды таңдалған жаңарту туралы жалпы мәліметтерді көрсетеді:

     - Жаңартуды мақұлдау күйі (ашылмалы тізімнен жаңа күйді таңдау арқылы қолмен өзгертуге болады).
     - Жаңарту тиесілі болып табылатын Windows Server Update Services (WSUS) қызметтер санаты.
     - Жаңартуды тіркеу күні мен уақыты.
     - Жаңартудың жасалған күні мен уақыты.
     - Жаңартудың маңыздылық деңгейі.
     - Жаңартуға қойылатын орнату талаптары.
     - Жаңарту кіретін бағдарламалар тобы.
     - Жаңарту қолданылатын бағдарлама.
     - Жаңартудың нұсқасының нөмірі.

   - **Атрибуттар**

     Бұл қойынды таңдалған жаңарту туралы қосымша ақпарат алу үшін пайдалануға болатын атрибуттар жиынтығын көрсетеді. Бұл жиынтық жаңартуды кім шығарғанына байланысты өзгереді: Microsoft немесе үшінші тарап өндірушісі.

     Қойынды Microsoft жаңартуы туралы келесі ақпаратты көрсетеді:

     - Microsoft Security Response Center (MSRC) талаптарына сәйкес жаңарту маңыздылығы деңгейі.
     - Жаңартуды сипаттайтын Microsoft білім базасындағы мақалаға сілтеме.
     - Жаңартуды сипаттайтын Microsoft Security Bulletin бюллетеніндегі мақалаға сілтеме.
     - Жаңарту идентификаторы (ID).

     Қойынды үшінші тарап өндірушісін жаңарту үшін келесі ақпаратты көрсетеді:

     - Жаңарту патч немесе толық дистрибутив болып табылады ма.
     - Жаңартудың локализация тілі.
     - Жаңарту автоматты түрде немесе қолмен орнатылады ма.

- Жаңарту қолданылғаннан кейін кері қайтарып алынды ма.
- Жаңартуды жүктеп алу сілтемесі.

- **Құрылғылар**

  Бұл қойынды таңдалған жаңарту орнатылған құрылғылардың тізімін көрсетеді.

- **Жабылатын осалдықтар**

  Бұл қойынды таңдалған жаңарту түзете алатын осалдықтардың тізімін көрсетеді.

- **Жаңартулардың қиылысу**

  Бұл қойындыда, бір бағдарлама үшін жарияланған түрлі жаңартулар арасындағы ықтимал қиылысулар көрсетіледі, яғни таңдалған жаңарту басқа жаңартуларды алмастыра алады ма немесе, керісінше, оны басқа жаңартулармен алмастыруға болады ма (Microsoft жаңартулары үшін ғана қолжетімді).

- **Жаңартуды орнату тапсырмалары**

  Бұл қойынды таңдалған жаңартуды орнатуды қамтитын тапсырмалар тізімін көрсетеді. Қойындыда жаңартуды қашықтан орнату тапсырмасын да жасауға болады.

Жаңартуды орнату статистикасын көру үшін:

1. Қажетті жаңартудың жанына жалаушаны қойыңыз.
2. **Жаңартуды орнату күйлерінің статистикасы** түймесін басыңыз.

Диаграмма жаңарту күйлері туралы ақпаратты көрсетеді. Күйді басу арқылы, жаңартудың таңдалған күйі бар құрылғылардың тізімі ашылады.

Сіз үшінші тарап бағдарламалары, соның ішінде таңдалған Windows басқарылатын құрылғысында орнатылған Microsoft бағдарламалық жасақтамасы үшін қолжетімді жаңартулар туралы ақпаратты көре аласыз.

Таңдалған басқарылатын құрылғы орнатылған үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін көру үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде үшінші тарап бағдарламаларының жаңартуларын көргіңіз келетін құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. Таңдалған құрылғы сипаттары терезесінде **Кеңейтілген** қойындысын таңдаңыз.
4. Сол жақ тақтадан **Қолжетімді жаңартулар** бөлімін таңдаңыз. Тек орнатылған жаңартуларды қарағыңыз келсе, **Орнатылған жаңартуларды көрсету** параметрін қосыңыз.

Таңдалған құрылғы үшін қолжетімді үшінші тарап бағдарламалық жасақтамасы жаңартуларының тізімі көрсетіледі.

Қолжетімді жаңартулар тізімін файлға экспорттау

Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламалары үшін көрсетілетін жаңартулар тізімін CSV немесе TXT пішіміндегі файлға экспорттауға болады. Сіз бұл файлдарды, мысалы, ақпараттық қауіпсіздік жөніндегі басшыңызға жіберу немесе статистика мақсатында сақтау үшін пайдалана аласыз.

Үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін барлық басқарылатын құрылғыларда орнатылған мәтіндік файлға экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Бетте барлық басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламалары үшін қолжетімді жаңартулардың тізімі көрсетілген.

2. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз.

Үшінші тарап бағдарламалары, соның ішінде Microsoft бағдарламалық жасақтамасы үшін қолжетімді жаңартулар тізімі бар файл сіз пайдаланып жатқан құрылғыға жүктеледі.

Үшінші тарап бағдарламалары үшін қолжетімді жаңартулар тізімін таңдалған басқарылатын құрылғыда орнатылған мәтіндік файлға экспорттау үшін:

1. Таңдалған басқарылатын құрылғыда қолжетімді үшінші тарап бағдарламалық жасақтама жаңартуларының тізімін ашыңыз.

2. Экспорттағыңыз келетін бағдарламалық жасақтама жаңартуларын таңдаңыз.

   Бағдарлама жаңартуларының толық тізімін экспорттағыңыз келсе, бұл қадамды өткізіп жіберіңіз.

   Бағдарлама жаңартуларының толық тізімін экспорттау кезінде тек ағымдағы бетте көрсетілетін жаңартулар экспортталады.

   Егер сіз тек орнатылған жаңартуларды экспорттағыңыз келсе, **Орнатылған жаңартуларды көрсету** жалаушасын қойыңыз.

3. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз.

Таңдалған басқарылатын құрылғыларда орнатылған Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламаларын жаңарту тізімі бар файл қазіргі уақытта пайдаланып жатқан құрылғыға жүктеледі.

Үшінші тарап бағдарламаларының жаңартуларын мақұлдау және қабылдамау

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын конфигурациялау кезінде, сіз орнату үшін орнатылатын жаңартулар белгілі бір күйге ие болуы керек ереже жасай аласыз. Мысалы, жаңарту ережесі келесілерді орнатуға мүмкіндік береді:

- тек мақұлданған жаңартулар;
- тек мақұлданған жаңартулар мен белгісіз жаңартулар;
- жаңарту күйіне қарамастан барлық жаңартулар.

Орнату қажет болған жаңартуларды растай аласыз немесе орнатылмауы тиісті жаңартулардан бас тарта аласыз.

Жаңартуларды орнатуды басқарған кезде, аздаған жаңартулар үшін *Расталды* күйін қолданған жөн. Бірнеше жаңарту орнату үшін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасында конфигурациялауға болатын ережелерді қолданыңыз. *Расталды* күйін, ережелерде көрсетілген өлшемшарттарға сай келмейтін жаңартулар үшін ғана белгілеу ұсынылады. Жаңартулардың көп санын қолмен растау кезінде, Басқару серверінің өнімділігі төмендеп, бұл Басқару серверінің артық жүктелуіне әкелуі мүмкін.

Бір немесе бірнеше жаңартуды растау немесе болдырмау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Растау немесе қабылдамау қажет болған жаңартуларды таңдаңыз.

3. Таңдалған жаңартуды мақұлдау үшін **Бекіту** түймесін басыңыз немесе таңдалған жаңартуды қабылдамау үшін **Қабылдамау** түймесін басыңыз.

   Әдепкі бойынша, *Анықталмаған* мәні орнатылған.

Таңдалған жаңартуларда сіз көрсеткен күйлер бар.

Сондай-ақ, қажетті жаңарту сипаттарындағы күйді өзгертуге болады.

Жаңартуды мақұлдау немесе қабылдамау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама жаңартулары** бөліміне өтіңіз.

   Қолжетімді жаңартулар тізімі көрсетіледі.

2. Мақұлдау немесе қабылдамау қажет жаңартуды таңдаңыз.

   Жаңарту сипаттары терезесі ашылады.

3. **Жалпы** бөлімінде **Жаңартуды растау күйі** параметрін өзгертіп, жаңарту күйін таңдаңыз. *Расталды*, *Қабылданбады* немесе *Анықталмаған* күйін таңдауға болады.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған жаңартуларда сіз көрсеткен күйлер бар.

Үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін **Қабылданбады** күйін белгілеп жатсаңыз, бұл жаңартулар орнатылуы жоспарланған, бірақ әлі орнатылмаған құрылғыларға орнатылмайды. Жаңартулар әлдеқашан орнатылған құрылғыларда қала береді. Оларды жою қажет болса, мұны жергілікті түрде қолмен орындай аласыз.

Windows Update жаңартуларын синхрондау тапсырмасын жасау

Windows Update жаңартуларын синхрондау тапсырмасы, Осалдықтар мен патчтарды басқару лицензия болған кезде қолжетімді.

Басқару серверін WSUS сервері ретінде пайдалануды қаласаңыз, *Windows Update жаңартуларын синхрондау* тапсырмасы керек. Бұл жағдайда, Басқару сервері Windows жаңартуларын дерекқорға жүктейді және Желілік агенттерді қолдана отырып, клиент құрылғыларында Windows Update жаңартуларын орталықтандырылған режимде ұсынады. Егер желіде WSUS сервері пайдаланылмаса, онда әрбір клиент құрылғысы Microsoft жаңартуларын сыртқы серверлерден дербес жүктейді.

Windows Update жаңартуларын синхрондау тапсырмасы Microsoft серверлерінен тек метадеректерді ғана жүктейді. Жаңартуларды орнату тапсырмасын орындау кезінде Kaspersky Security Center бағдарламасы тек сіз таңдаған жаңартуларды жүктейді.

Windows Update жаңартуларын синхрондау тапсырмасын орындау барысында, бағдарлама Microsoft жаңартулар серверінен өзекті жаңартулар тізімін алады. Содан соң, Kaspersky Security Center бағдарламасы ескірген жаңартулар тізімін анықтайды. **Осалдықтарды және қажетті жаңартуларды іздеу** тапсырмасын келесі жолы іске қосқан кезде, Kaspersky Security Center бағдарламасы ескірген жаңартуларды белгілеп, жою уақытын белгілейді. **Windows Update жаңартуларын синхрондау** тапсырмасын келесіде іске қосқан кезде, 30 күн бұрын жою жалаушасы қойылған барлық жаңарту жойылады. Kaspersky Security Center 180 күннен артық уақыт бұрын жою жалаушасы қойылған ескі жаңартуларды да тексеріп, оларды жояды.

Windows Update жаңартуларын синхрондау тапсырмасының жұмысы аяқталғаннан және дерекқорларда ескірген жаңартулар жойылғаннан кейін, жойылған жаңартулар файлдарының хеш-кодтары, сондай-ақ олар бұған дейін жүктелген болса, %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles қалтасында оларға сай келетін файлдар қалып қоюы мүмкін. **Басқару серверіне техникалық қызмет көрсету** тапсырмасының көмегімен мұндай ескірген жазбаларды дерекқордан және оларға сай келетін файлдардан жоюға болады.

Windows Update жаңартуларын синхрондау тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Kaspersky Security Center бағдарламасы үшін **Windows Update жаңартуларын синхрондау** тапсырма түрін таңдаңыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

5. Экспресс-жаңарту файлдары тапсырманы орындау кезінде жүктелгенін қаласаңыз, **Жылдам орнату файлдарын жүктеп алу** параметрін қосыңыз.

   Kaspersky Security Center бағдарламасы жаңартуларды Microsoft Windows Update Servers серверлерімен синхрондағанда, барлық файлдар туралы ақпарат Басқару серверінің дерекқорында сақталады. Сондай-ақ, дискіге Windows жаңарту агентімен өзара әрекеттесу кезінде жаңартуға қажетті барлық файлдар жүктеледі. Атап айтқанда, Kaspersky Security Center жедел орнату файлдары туралы ақпаратты дерекқорға сақтайды және қажет болған жағдайда жүктейді. Жедел орнату файлдарын жүктеу дискідегі бос орынды қысқартуға себеп болады.

   Диск кеңістігі көлемінің қысқаруын азайту және трафикті төмендету үшін **Жылдам орнату файлдарын жүктеп алу** параметрін өшіріңіз.

6. Жаңартуларды жүктеп алу қажет болып саналатын бағдарламаларды таңдаңыз.

   Барлық бағдарламалар жалаушасы қойылған болса, онда жаңартулар барлық қолданыстағы бағдарламалар үшін, сондай-ақ болашақта шығарылуы мүмкін бағдарламалар үшін жүктеледі.

7. Басқару серверіне жүктегіңіз келетін жаңартулар санатын таңдаңыз.

   Барлық санаттар жалаушасы қойылған болса, онда жаңартулар барлық қолданыстағы жаңарту санаттары үшін, сондай-ақ болашақта пайда болуы мүмкін санаттар үшін жүктеледі.

8. Басқару серверіне жүктегіңіз келетін жаңартуларды локализациялау тілдерін таңдаңыз. Келесі нұсқалардың бірін таңдаңыз:

   - **Барлық тілдерді, соның ішінде жаңаларын жүктеп алу**

     Егер бұл нұсқа таңдалса, жаңартулардың барлық қолжетімді локализация тілдері Басқару серверіне жүктеледі. Әдепкі бойынша, осы нұсқа таңдалған.

   - **Таңдалған тілдерді жүктеп алу**

     Егер бұл нұсқа таңдалса, тізімде Басқару серверіне жүктелетін жаңартулардың локализация тілдерін таңдауға болады.

9. Тапсырманы қандай есептік жазбамен іске қосу керектігін көрсетіңіз. Келесі нұсқалардың бірін таңдаңыз:

   - **Әдепкі есептік жазба**

     Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Есептік жазбаны көрсету**

     Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

10. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

11. **Аяқтау** түймесін басыңыз.

    Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

12. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

13. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіңіз.

14. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Үшінші тарап бағдарламаларын автоматты түрде жаңарту

Кейбір үшінші тарап бағдарламалары автоматты түрде жаңартылуы мүмкін. Бағдарлама өндірушісі бағдарламаның автоматты түрде жаңарту функциясын қолдайтынын анықтайды. Егер басқарылатын құрылғыда орнатылған үшінші тарап бағдарламасы автоматты түрде жаңартуды қолдаса, бағдарлама сипаттарында автоматты түрде жаңарту параметрін көрсетуге болады. Автоматты жаңарту параметрін өзгерткеннен кейін, Желілік агенттер бағдарлама орнатылған әрбір басқарылатын құрылғыда жаңа параметрді қолданады.

Автоматты жаңарту параметрі басқа нысандарға және Осалдықтар мен патчтарды басқару мүмкіндіктеріне тәуелді емес. Мысалы, бұл параметр *Қажетті жаңартуларды орнату және осалдықтарды түзету*, *Windows Update жаңартуларын орнату* және *Осалдықтарды түзету* сияқты жаңартуды мақұлдау күйіне немесе жаңартуды орнату тапсырмаларына байланысты емес.

Үшінші тарап бағдарламасына арналған автоматты жаңарту параметрін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Автоматты жаңарту параметрін өзгерткіңіз келетін бағдарламаның атын басыңыз.

   Іздеуді жеңілдету үшін, тізімді **Автоматты жаңартулар күйі** бағаны бойынша сүзуге болады.

   Бағдарлама сипаттары терезесі ашылады.

3. **Жалпы** бөлімінде келесі параметр үшін мәнді таңдаңыз:

   Автоматты жаңартулар күйі

   Келесі нұсқалардың бірін таңдаңыз:

   - **Анықталмаған**

     Автоматты жаңарту функциясы өшірулі. Kaspersky Security Center бағдарламасы үшінші тарап бағдарламаларының жаңартуларын *Қажетті жаңартуларды орнату және осалдықтарды түзету*, *Windows Update жаңартуларын орнату* және *Осалдықтарды түзету* арқылы орнатады.

   - **Рұқсат етілген**

     Өндіруші бағдарлама үшін жаңартуды шығарғаннан кейін, бұл жаңарту автоматты түрде басқарылатын құрылғыларға орнатылады. Қосымша әрекеттер керек емес.

- **Бұғатталған**

  Бағдарлама жаңартулары автоматты түрде орнатылмайды. Kaspersky Security Center бағдарламасы үшінші тарап бағдарламаларының жаңартуларын *Қажетті жаңартуларды орнату және осалдықтарды түзету*, *Windows Update жаңартуларын орнату* және *Осалдықтарды түзету* арқылы орнатады.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Автоматты жаңарту конфигурациясы таңдалған бағдарламаға қолданылады.

Үшінші тарап бағдарламаларында осалдықтарды түзету

Бұл бөлімде, басқарылатын құрылғыларда орнатылған бағдарламаларда осалдықтарды түзетумен байланысты Kaspersky Security Center мүмкіндіктері сипатталған.

Сценарий: Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету

Бұл бөлімде, Windows басқаруымен жұмыс істейтін құрылғылардағы осалдықтарды анықтау және түзету сценарийі келтірілген. Операциялық жүйелердегі, үшінші тарап бағдарламаларындағы, соның ішінде Microsoft бағдарламаларындағы осалдықтарды анықтауға және түзетуге болады.

Алдын ала талаптар

- Kaspersky Security Center бағдарламасы сіздің ұйымыңызда орналастырылған.
- Ұйымыңыздың желісінде Windows басқаруымен жұмыс істейтін басқарылатын құрылғылар бар.
- Басқару серверін интернетке қосу келесі тапсырмаларды орындау үшін қажет:
  - Microsoft бағдарламалық жасақтама осалдықтарының ұсынылған түзетулер тізімін жасау. Тізімді Kaspersky мамандары қалыптастырады және үнемі жаңартып отырады.
  - Microsoft бағдарламаларынан басқа үшінші тарап бағдарламаларындағы осалдықтарды түзету.

Кезеңдер

Осалдықтарды анықтау және түзету келесі кезеңдерден тұрады:

1. **Басқарылатын құрылғыларда орнатылған бағдарламалық жасақтамадағы осалдықтарды іздеу**

   Басқарылатын құрылғыларда орнатылған бағдарламалардағы осалдықтарды табу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын іске қосыңыз. Бұл тапсырма аяқталғаннан кейін, Kaspersky Security Center бағдарламасы құрылғыларға орнатылған және тапсырма сипаттарында көрсетілген үшінші тарап бағдарламалары үшін қажетті жаңартулар мен табылған осалдықтар тізімдерін алады.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Бағдарламаны жылдам іске қосу шеберін іске қоспаған болсаңыз, оны қазір іске қосыңыз немесе тапсырманы қолмен жасаңыз.

Нұсқаулар:

- Басқару консолі: Бағдарламаларда осалдықтарды іздеу, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы үшін кестені белгілеу.
- Kaspersky Security Center Web Console: Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасын жасау, Осалдықтар мен қажетті жаңартуларды іздеу тапсырмасы параметрлері.

2. **Анықталған бағдарламалық жасақтама осалдықтары тізімін талдау**

Бағдарламалық жасақтама осалдықтары тізімін қарап, қандай осалдықтарды түзету керектігін шешіңіз. Әрбір осалдық туралы толық ақпаратты көру үшін тізімдегі осалдық атауын басыңыз. Тізімдегі әрбір осалдық үшін басқарылатын құрылғылардағы осалдық статистикасын да көруге болады.

Нұсқаулар:

- Басқару консолі: Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау, Басқарылатын құрылғылардағы осалдықтар статистикасын қарау.
- Kaspersky Security Center Web Console: Бағдарламалық жасақтама осалдықтары туралы ақпаратты қарау, Басқарылатын құрылғылардағы осалдықтар статистикасын қарау.

3. **Осалдықты түзетуді конфигурациялау**

Бағдарламаларда осалдықтарды анықтап, сіз *Қажетті жаңартуларды орнату және осалдықтарды түзету* немесе *Осалдықтарды түзету* тапсырмасын қолдану арқылы басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын түзете аласыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, үшінші тарап бағдарламаларында, соның ішінде басқарылатын құрылғыларға орнатылған Microsoft бағдарламаларында жаңарту және осалдықтарды түзету үшін қолданылады. Бұл тапсырма бірнеше жаңартуларды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықтарды түзетуге мүмкіндік береді. Назар аударыңыз, Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса ғана осы тапсырманы жасауға болады. Бағдарламалық жасақтама осалдықтарын түзету үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы ұсынылған бағдарламалық жасақтама жаңартуларын қолданады.

Осалдықтарды түзету тапсырмасы Осалдықтар мен патчтарды басқару үшін лицензияны қажет етпейді. Бұл тапсырманы пайдалану мақсатында, тапсырма параметрлерінде көрсетілген үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін пайдаланушылық түзетулерді қолмен көрсету қажет. *Осалдықтарды түзету* тапсырмасы үшінші тарап бағдарламалары үшін ұсынылған Microsoft бағдарламаларының түзетулері мен пайдаланушылық түзетулерді пайдаланады.

Сіз осы тапсырмалардың бірін автоматты түрде жасайтын осалдықтарды түзету шеберін іске қоса аласыз немесе сол тапсырмалардың бірін қолмен жасай аласыз.

Нұсқаулар:

- Басқару консолі: Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушылық түзетулер, Бағдарламалық жасақтама осалдықтарын түзету.
- Kaspersky Security Center Web Console: Үшінші тарап бағдарламаларындағы осалдықтар үшін пайдаланушылық түзетулер, Үшінші тарап бағдарламаларындағы осалдықтарды түзету, Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау.

4. **Тапсырманың кестесін белгілеу**

Осалдықтар тізімі әрқашан өзекті екеніне көз жеткізу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасының іске қосылу кестесін белгілеңіз, сонда ол мезгіл-мезгіл автоматты түрде іске қосылады. Ұсынылатын орташа кезең – аптасына бір рет.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасаған болсаңыз, оны іске қосуды *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасына арналған жиілікпен немесе одан сирек жиілікпен іске қосуды белгілей аласыз. *Осалдықтарды түзету* тапсырмасының кестесін белгілеген кезде, тапсырманы іске қоспас бұрын Microsoft бағдарламаларының түзетулерін таңдау немесе үшінші тарап бағдарламалары үшін арнайы түзетулерді көрсету керек.

Тапсырмалар кестесін белгілеу кезінде, осалдықтарды түзету тапсырмасы *Осалдықтарды және қажетті жаңартуларды іздеу* аяқталғаннан кейін іске қосылатынына көз жеткізіңіз.

5 Бағдарламалық жасақтама осалдықтарын елемеу (қажет болса)

Барлық басқарылатын құрылғыларда немесе тек таңдалған басқарылатын құрылғыларда түзетілуі тиісті бағдарламалардағы осалдықты елемеуге болады.

Нұсқаулар:

- Басқару консолі: Бағдарламалардағы осалдықтарды елемеу.
- Kaspersky Security Center Web Console: Бағдарламалық жасақтама осалдықтарын елемеу.

6 Осалдықтарды түзету тапсырмасын іске қосу

Қажетті жаңартуларды орнату және осалдықтарды түзету немесе *Осалдықты түзету* тапсырмасын іске қосыңыз. Тапсырма аяқталғаннан кейін, оның тапсырмалар тізімінде *Сәтті аяқталды* күйі бар екеніне көз жеткізіңіз.

7 Бағдарламалық жасақтама осалдықтарын түзету нәтижелері туралы есеп жасау (қажет болса)

Жабық осалдықтар туралы статистиканы көру үшін осалдықтар туралы есепті жасаңыз. Есепте түзетілмеген бағдарламалық жасақтама осалдықтары туралы ақпарат көрсетіледі. Осылайша, сіз өзіңіздің ұйымыңыздағы үшінші тарап бағдарламаларындағы, соның ішінде Microsoft бағдарламалық жасақтамасындағы осалдықтарды анықтау және түзету туралы түсінікке ие бола аласыз.

Нұсқаулар:

- Басқару консолі: Есепті жасау және қарау
- Kaspersky Security Center Web Console: Есепті жасау және қарау

8 Үшінші тарап бағдарламаларындағы осалдықтарды анықтау және түзету параметрлерін тексеру

Келесіні орындағаныңызға көз жеткізіңіз:

- басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтары тізімін тауып, қарап шыққаныңызға;
- егер қаласаңыз, бағдарламалардағы осалдықтарды елемегеніңізге;
- осалдықты түзету тапсырмасын конфигурациялағаныңызға;
- бағдарламалардағы осалдықтарды іздеуге және түзетуге арналған тапсырмаларды дәйекті түрде іске қосылатындай етіп іске қосуды жоспарлады;
- осалдықтарды түзету міндеті іске қосылғанын тексерді.

Нәтижелер

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасасаңыз және конфигурацияласаңыз, осалдықтар басқарылатын құрылғыларда автоматты түрде жабылады. Тапсырманы іске қосу кезінде тапсырма қолжетімді бағдарламалық жасақтама жаңартуларының тізімін тапсырма параметрлерінде көрсетілген ережелермен салыстырады. Ережелердегі критерийлерге сәйкес келетін барлық бағдарламалық жасақтама жаңартулары Басқару сервері қоймасына жүктеледі және бағдарламалардағы осалдықтарды түзету үшін орнатылады.

Осалдықтарды түзету тапсырмасын жасаған болсаңыз, Microsoft бағдарламаларындағы осалдықтар ғана түзетіледі.

Бағдарламалық жасақтама осалдықтарын анықтау және түзету туралы

Kaspersky Security Center бағдарламасы Microsoft Windows операциялық жүйелерінің басқаруымен жұмыс істейтін басқарылатын құрылғылардағы бағдарламаларда осалдықтарды анықтайды және түзетеді. Осалдықтар операциялық жүйелерде және Microsoft бағдарламалық жасақтамасын қоса, үшінші тарап бағдарламаларында кездеседі.

Жаңарту функционалдығы (антивирустық қолтаңба жаңартуларын және код дерекқоры жаңартуларын қоса) және KSN функционалдығы АҚШ аймағындағы бағдарламада қолжетімді болмауы мүмкін.

Бағдарламалық жасақтама осалдықтарын анықтау

Осалдықтарды анықтау үшін Kaspersky Security Center бағдарламасы белгілі осалдықтар туралы дерекқордағы белгілерге негізделген бағдарламалық жасақтаманың белгілі осалдықтарын іздейді. Бұл дерекқорды Kaspersky мамандары қалыптастырады. Онда осалдықтардың сипаттамасы, осалдықтарды анықтау күні, осалдықтардың қауіптілік деңгейі сияқты осалдықтар туралы ақпарат бар. Сіз осалдықтар туралы мәліметті Kaspersky сайтынан ала аласыз.

Kaspersky Security Center бағдарламасында бағдарламалардың осалдықтардың іздеу үшін *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы қолданылады.

Кейбір жағдайларда Microsoft Windows операциялық жүйесінде анықталған осалдықтарды келесі тәсілдердің бірі арқылы жоюға болады:

- Операциялық жүйе үшін жаңартуларды орнатыңыз.
- Операциялық жүйені жаңа нұсқаға жаңартыңыз (мысалы, Windows 10-дан Windows 11-ге дейін).

Бұл сценарийде Kaspersky Security Center бірдей осалдық үшін екі жазбаны көрсетеді.

Бағдарламаларда осалдықты түзету

Бағдарламаларда осалдықтарды түзету үшін, Kaspersky Security Center бағдарламасы бағдарламалық жасақтама өндірушілері шығарған бағдарламалық жасақтама жаңартуларын қолданады. Бағдарламалық жасақтаманы жаңарту метадеректері келесі тапсырмаларды орындау нәтижесінде Басқару сервері қоймасына жүктеледі:

- *Жаңартуларды Басқару серверінің қоймасына жүктеп алу*. Бұл тапсырма Kaspersky бағдарламалары мен үшінші тарап бағдарламалары үшін жаңарту метадеректерін жүктеуге арналған. Бұл тапсырма Kaspersky Security Center бағдарламаны жылдам іске қосу шеберінде автоматты түрде жасалады. Жаңартуларды Басқару серверінің қоймасына жүктеп алу тапсырмасын қолмен жасауға болады.

- *Windows Update жаңартуларын синхрондау*. Бұл тапсырма Microsoft бағдарламалық жасақтамасының жаңартуларының метадеректерін жүктеуге арналған.

Осалдықтарды түзетуге арналған бағдарламалық жасақтаманың жаңартулары толық дистрибутивтер немесе патчтар түрінде ұсынылуы мүмкін. Бағдарламалық жасақтаманың осалдықтарын түзететін бағдарламалық жасақтама жаңартулары *түзетулер* деп аталады. *Ұсынылған түзетулер* – бұл Kaspersky мамандары орнатуға ұсынатын түзетулер. *Пайдаланушылық түзетулер* – бұл пайдаланушылар орнату үшін қолмен көрсетілетін түзетулер. Пайдаланушылық түзетулерді орнату үшін осы түзетуді қамтитын орнату пакетін жасау керек.

Kaspersky Security Center лицензиясы Осалдықтар мен патчтарды басқару мүмкіндіктерін көздесе, осалдықтарды түзету үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын пайдаланыңыз. Бұл тапсырма ұсынылған түзетулерді орнату арқылы бірнеше осалдықтарды автоматты түрде түзетеді. Бұл тапсырма үшін бірнеше осалдықтарды түзету үшін белгілі бір ережелерді қолмен конфигурациялауға болады.

Kaspersky Security Center лицензиясы Осалдықтар мен патчтарды басқару мүмкіндіктерін көздемесе, осалдықтарды түзету үшін *Осалдықтарды түзету* тапсырмасын пайдаланыңыз. Бұл тапсырманың көмегімен Microsoft бағдарламалары үшін ұсынылған түзетулерді және үшінші тарап бағдарламалары үшін пайдаланушылық түзетулерді орнату арқылы осалдықтарды түзетуге болады.

Қауіпсіздік мақсатында, Осалдықтар мен патчтарды басқару арқылы орнатқан кез келген үшінші тарап бағдарламалық жасақтамасы жаңартулары Kaspersky технологиялары арқылы зиянды БҚ-дың бар-жоғы тұрғысынан автоматты түрде тексеріледі. Бұл технологиялар файлдарды автоматты түрде тексеру үшін қолданылады және антивирустық тексеруді, статикалық талдауды, динамикалық талдауды, "құмсалғыштың" жүріс-тұрысын талдауды және машиналық оқытуды қамтиды.

Kaspersky мамандары Осалдықтар мен патчтарды басқару арқылы орнатуға болатын үшінші тарап бағдарламалық жасақтамасы жаңартуларын қолмен талдамайды. Сонымен қатар Kaspersky мамандары мұндай жаңартулардағы осалдықтарды (белгілі немесе белгісіз) немесе құжатталмаған мүмкіндіктерді іздеумен айналыспайды және жоғарыда аталған талдаудың басқа түрлерін жүргізбейді.

> Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Бағдарламалық жасақтаманың кейбір осалдықтарын түзету үшін, қажет болса, бағдарламалық жасақтаманы орнатуға арналған лицензиялық келісімді қабылдау керек. Егер сіз Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтаманың осалдығы түзетілмейді.

Үшінші тарап бағдарламаларында осалдықтарды түзету

Бағдарламаларда осалдықтар тізімін алғаннан кейін, Windows операциялық жүйелері бар басқарылатын құрылғылардағы бағдарламаларда осалдықтарды түзете аласыз. *Осалдықтарды түзету* тапсырмасын немесе *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасау және іске қосу арқылы Microsoft бағдарламалық жасақтамасын қоса отырып, үшінші тарап бағдарламалары мен операциялық жүйеде осалдықтарды түзете аласыз.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Сондай-ақ, бағдарламалардағы осалдықтарды түзету үшін тапсырманы келесі жолдармен жасауға болады:

- Осалдықтар тізімін ашып, қандай осалдықтарды түзету керектігін көрсетіңіз.

  Нәтижесінде, бағдарламалардағы осалдықтарды түзету тапсырмасы туындайды. Таңдалған осалдықтарды қолданыстағы тапсырмаға қосуға болады.

- Осалдықтарды түзету шеберін іске қосыңыз.

  Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері қолжетімді болады.

  Шебер осалдықтарды түзету тапсырмасын құруды және конфигурациялауды жеңілдетеді, сонымен қатар орнату үшін бірдей жаңартулары бар артық тапсырмаларды құруды болдырмайды.

Бағдарламалардағы осалдықтарды осалдықтар тізімімен түзету

Бағдарламалардағы осалдықтарды түзету үшін:

1. Осалдық тізімдерінің бірін ашыңыз:

   - Жалпы осалдықтар тізімін ашу үшін, басты мәзірде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   - Басқарылатын құрылғының осалдықтар тізімін ашу үшін, басты мәзірде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** → <құрылғы атауы> → **Кеңейтілген** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   - Қажетті бағдарламаның осалдықтар тізімін ашу үшін, басты мәзірде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** → <бағдарлама атауы> → **Осалдықтар** бөліміне өтіңіз.

   Үшінші тарап бағдарламаларында осалдықтар тізімі бар бет көрсетіледі.

2. Тізімдегі бір немесе бірнеше осалдықтарды таңдап, **Осалдықты түзету** түймесін басыңыз.

   Таңдалған осалдықтардың бірін түзету үшін ұсынылған бағдарламалық жасақтамасының жаңартуы болмаса, ақпараттық хабар көрсетіледі.

Бағдарламалық жасақтаманың кейбір осалдықтарын түзету үшін, қажет болса, бағдарламалық жасақтаманы орнатуға арналған лицензиялық келісімді қабылдау керек. Егер сіз Лицензиялық келісімнен бас тартсаңыз, бағдарламалық жасақтаманың осалдығы түзетілмейді.

3. Келесі нұсқалардың бірін таңдаңыз:

   - **Жаңа тапсырма**

     Жаңа тапсырма жасау шебері іске қосылады. Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, әдепкі бойынша *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырма түрі таңдалады. Лицензияңыз болмаса, әдепкі бойынша *Осалдықтарды түзету* тапсырма түрі таңдалады. Тапсырма жасауды аяқтау үшін шебердің алдағы нұсқауларын орындаңыз.

   - **Осалдықты түзету (көрсетілген тапсырмаға ереже қосу)**

     Осалдықтардың таңдаулылар тізіміне қосқыңыз келетін тапсырманы таңдаңыз. Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болса, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын таңдаңыз. Таңдалған тапсырмаға таңдалған осалдықтарды түзетуге арналған жаңа ереже автоматты түрде қосылады. Лицензияңыз болмаса, әдепкі бойынша *Осалдықтарды түзету* тапсырма түрі таңдалады. Таңдалған осалдықтар тапсырма сипаттарына қосылады.

     Тапсырма сипаттары терезесі ашылады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Тапсырма жасауды таңдаған болсаңыз, ол тапсырмалар тізімінде, **Активтер (құрылғылар)** → **Тапсырмалар** бөлімінде жасалып, көрсетіледі Егер сіз бар тапсырмаға осалдықтарды қосуды таңдасаңыз, осалдықтар тапсырма сипаттарында сақталады.

Үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* немесе *Осалдықтарды түзету* тапсырмаларын іске қосыңыз. *Осалдықтарды түзету* тапсырмасын жасаған болсаңыз, сіз тапсырманың сипаттарында атап көрсетілген осалдықтарды түзету үшін бағдарламалық жасақтаманың осалдықтарын қолмен көрсетуіңіз керек.

Осалдықтарды түзету шебері арқылы бағдарламалардағы осалдықтарды түзету

Осалдықтар мен патчтарды басқару үшін лицензия болған кезде, осалдықтарды түзету шебері қолжетімді болады.

Осалдықтарды түзету шебері арқылы бағдарламалардағы осалдықтарды түзету үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Патчтарды басқару** → **Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда орнатылған үшінші тарап бағдарламаларындағы осалдықтар тізімі бар бет ашылады.

2. Түзетуді қажет ететін осалдыққа қарсы жалауша қойыңыз.

3. **Осалдықтарды түзету шеберін іске қосу** түймесін басыңыз.

Осалдықтарды түзету шебері ашылады. **Осалдықты түзету тапсырмасын таңдау** бетінде келесі түрдегі барлық қолданыстағы тапсырмалар тізімі көрсетіледі:

- *Қажетті жаңартуларды орнату және осалдықтарды түзету*
- *Windows Update жаңартуларын орнату*
- *Осалдықтарды түзету*

Жаңа жаңартуларды орнату үшін тапсырмалардың соңғы екі түрін өзгерту мүмкін емес. Жаңа жаңартуларды орнату үшін *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын ғана қолдануға болады.

4. Егер сіз шебердің таңдалған осалдықты түзететін тапсырмаларды ғана көрсетуін қаласаңыз, **Осы осалдықты түзететін тапсырмаларды ғана көрсету** параметрін қосыңыз.

5. Орындағыңыз келетін әрекетті таңдаңыз:

   - Тапсырманы іске қосу үшін, тапсырманың аты жанында жалаушаны қойып, **Іске қосу** түймесін басыңыз.
   - Қолданыстағы тапсырмаға жаңа ережені қосу үшін:

     a. Тапсырманың аты жанына жалаушаны қойып, **Ереже қосу** түймесін басыңыз.

     b. Ашылған бетте жаңа ережені орнатыңыз:

     - **Осы күрделілік деңгейіндегі осалдықтарды түзету ережесі**

       Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

       Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

       Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

       Әдепкі бойынша, параметр өшірулі.

     - **Таңдалған осалдыққа арналған нұсқауларға сәйкес анықталған жаңарту түріндегі жаңартулармен осалдықтарды түзету ережесі** (тек Microsoft бағдарламаларындағы осалдықтар үшін қолжетімді)
     - **Таңдалған жеткізуші бойынша бағдарламаларда осалдықтарды түзету ережесі** (үшінші тарап бағдарламаларындағы осалдықтар үшін ғана қолжетімді)
     - **Таңдалған бағдарламаның барлық нұсқаларында осалдықты түзету ережесі** (үшінші тарап бағдарламаларындағы осалдықтар үшін ғана қолжетімді)
     - **Таңдалған осалдықты түзету ережесі**
     - **Осы осалдықты түзететін жаңартуларды растау**

       Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

Әдепкі бойынша, параметр өшірулі.

c. **Қосу** түймесін басыңыз.

- Тапсырма жасау үшін:

a. **Жаңа тапсырма** түймесін басыңыз.

b. Ашылған бетте жаңа ережені орнатыңыз:

- **Осы күрделілік деңгейіндегі осалдықтарды түзету ережесі**

  Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

  Егер бұл параметр қосулы болса, жаңартулар тек Kaspersky орнатқан критикалық деңгейі таңдалған жаңартудың маңыздылық мәніне тең немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары** немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

  Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

  Әдепкі бойынша, параметр өшірулі.

- **Таңдалған осалдыққа арналған нұсқауларға сәйкес анықталған жаңарту түріндегі жаңартулармен осалдықтарды түзету ережесі** (тек Microsoft бағдарламаларындағы осалдықтар үшін қолжетімді)

- **Таңдалған жеткізуші бойынша бағдарламаларда осалдықтарды түзету ережесі** (үшінші тарап бағдарламаларындағы осалдықтар үшін ғана қолжетімді)

- **Таңдалған бағдарламаның барлық нұсқаларында осалдықты түзету ережесі** (үшінші тарап бағдарламаларындағы осалдықтар үшін ғана қолжетімді)

- **Таңдалған осалдықты түзету ережесі**

- **Осы осалдықты түзететін жаңартуларды растау**

  Таңдалған жаңарту орнатуға мақұлданған. Егер жаңартуды орнатудың кейбір ережелері тек мақұлданған жаңартуларды орнатуға мүмкіндік берсе, бұл параметр қолжетімді.

  Әдепкі бойынша, параметр өшірулі.

c. **Қосу** түймесін басыңыз.

Егер сіз тапсырманы іске қосуды шешсеңіз, шеберді жабуға болады. Тапсырма фондық режимде орындалады. Қосымша әрекеттер қажет емес.

Егер сіз бар тапсырмаға ереже қосуды таңдасаңыз, тапсырма сипаттары терезесі ашылады. Тапсырманың сипаттарына жаңа ереже қосылды. Ережені, сондай-ақ басқа тапсырма параметрлерін көруге немесе өзгертуге болады. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Тапсырма жасауды шешсеңіз, оны тапсырма жасау шеберінің көмегімен жасаңыз. Осалдықтарды түзету шеберіне қосылған жаңа ереже тапсырманы жасау шеберінде көрсетіледі. Шебердің жұмысы аяқталғаннан кейін, *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы тапсырмалар тізіміне қосылады.

Осалдықтарды түзету тапсырмасын жасау

Осалдықтарды түзету тапсырмасы Windows операциялық жүйелері бар басқарылатын құрылғылардағы бағдарламалардағы осалдықтарды түзетуге мүмкіндік береді. Microsoft бағдарламалық жасақтамасын қоса алғанда, үшінші тарап бағдарламалары осалдықтарын түзете аласыз.

Осалдықтар мен патчтарды басқаруға арналған лицензияңыз болмаса, сіз *Осалдықтарды түзету* түріндегі тапсырмаларды жасай аласыз. Жаңа осалдықтарды түзету үшін, сіз оларды бұрыннан бар *Осалдықтарды түзету* тапсырмасына қоса аласыз. *Осалдықтарды түзетуҚажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы орнына Қажетті жаңартуларды орнату және осалдықтарды түзетуОсалдықтарды түзету* тапсырмасын қолдану ұсынылады. *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы автоматты түрде бірнеше жаңартуды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықты түзетуге мүмкіндік береді.

Пайдаланушының араласуы үшінші тарап бағдарламаларын жаңарту кезінде немесе басқарылатын құрылғыдағы үшінші тарап бағдарламаларында осалдықтарды түзету кезінде қажет болуы мүмкін. Мысалы, пайдаланушыдан үшінші тарап бағдарламасын жабу сұралуы мүмкін.

Осалдықтарды түзету тапсырмасын жасау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Kaspersky Security Center бағдарламасы үшін **Осалдықтарды түзету** тапсырма түрін таңдаңыз.
4. Жасап жатқан тапсырманың атын көрсетіңіз.

   Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.
5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.
6. **Қосу** түймесін басыңыз.

   Осалдықтар тізімі ашылады.
7. Жапқыңыз келетін осалдықтарды таңдап, **OK** түймесін басыңыз.

   Microsoft бағдарламалық жасақтамасының осалдықтары үшін әдетте ұсынылған түзетулер бар. Олар үшін қосымша әрекеттер қажет емес. Үшінші тарап бағдарламалары осалдықтары үшін алдымен түзеткіңіз келетін әрбір осалдық үшін пайдаланушы түзетуін көрсету керек. Содан соң, сіз осы осалдықтарды *Осалдықтарды түзету* тапсырмасына қоса аласыз.
8. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

   - **Құрылғыны қайта іске қоспау**

     Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сұрауды қайталау жиілігі (мин)**

  Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

  Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

- **Келесі уақыттан кейін қайта іске қосу (мин)**

  Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сеанстардағы бағдарламалардың мәжбүрлі жабылуы**

  Іске қосылған қолданбалар клиент құрылғысын қайта жүктеуге мүмкіндік бермеуі мүмкін. Мысалы, егер мәтіндік редакторда құжатпен жұмыс жасалса және өзгертулер сақталмаса, бағдарлама құрылғыны қайта жүктеуге мүмкіндік бермейді.

  Егер бұл параметр қосулы болса, құрылғыны қайта іске қоспас бұрын бұғатталған құрылғылардағы мұндай бағдарламалар мәжбүрлі түрде жабылады. Нәтижесінде, пайдаланушылар сақталмаған жұмысын жоғалтуы мүмкін.

  Егер бұл параметр өшірулі болса, бұғатталған құрылғы қайта жүктелмейді. Бұл құрылғыдағы тапсырманың күйі құрылғыны қайта іске қосу қажеттілігін көрсетеді. Пайдаланушылар бұғатталған құрылғыларда жұмыс істейтін барлық бағдарламаларды қолмен жауып, сол құрылғыларды қайта іске қосуы керек.

  Әдепкі бойынша, параметр өшірулі.

9. Есептік жазба параметрлерін белгілеңіз:

- **Әдепкі есептік жазба**

  Тапсырма, сол тапсырманы орындайтын бағдарлама орнатылған және іске қосылған сол есептік жазбамен іске қосылады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Есептік жазбаны көрсету**

  Есептік жазба және **Құпиясөз** өрістерінде тапсырма іске қосылуы тиісті есептік жазба деректерін көрсетіңіз. Есептік жазбада тапсырманы орындау үшін қажетті құқықтар болуы керек.

- **Есептік жазба**

  Тапсырманы іске қосатын есептік жазба.

- **Құпиясөз**

  Тапсырманы іске қосатын есептік жазбаның құпиясөзі.

10. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

11. **Аяқтау** түймесін басыңыз.

    Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

12. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

13. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіңіз.

14. **Сақтау** түймесін басыңыз.

Тапсырма жасалды және конфигурацияланды.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, Осалдықтар мен патчтарды басқару лицензия болған кезде қолжетімді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасы, үшінші тарап бағдарламаларында, соның ішінде басқарылатын құрылғыларға орнатылған Microsoft бағдарламаларында жаңарту және осалдықтарды түзету үшін қолданылады. Бұл тапсырма бірнеше жаңартуларды орнатуға және белгіленген ережелерге сәйкес бірнеше осалдықтарды түзетуге мүмкіндік береді.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасының көмегімен жаңартуларды орнату немесе осалдықтарды түзету үшін, сіз келесі әрекеттердің бірін орындай аласыз:

- Жаңартуды орнату шеберін немесе осалдықтарды түзету шеберін іске қосыңыз.
- *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасаңыз.
- Қолданыстағы *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасына жаңартуды орнату ережесін қосыңыз.

Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау үшін:

1. Қолданбаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. Kaspersky Security Center бағдарламасы үшін **Қажетті жаңартуларды орнату және осалдықтарды түзету** тапсырма түрін таңдаңыз.

   Тапсырма көрсетілмесе, есептік жазбада **Жүйені басқару**: **Осалдықтар мен патчтарды басқару** функционалды аймағына арналған **Оқу**, **өзгерту** және **орындау** құқықтары бар екенін тексеріңіз. Сіз осы қатынас құқықтарынсыз *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын жасай алмайсыз және конфигурациялай алмайсыз.

4. Жасап жатқан тапсырманың атын көрсетіңіз. Тапсырма атауы 100 таңбадан асуы және арнайы таңбаларды ("*<>?\:|) қамтуы мүмкін емес.

5. Тапсырмалар тағайындалатын құрылғыларды таңдаңыз.

6. Жаңартуларды орнату ережелерін, содан соң келесі параметрлерді көрсетіңіз:

   - **Орнатуды құрылғыны қайта жүктеу немесе өшіру сәтінде бастау**

     Егер жалауша қойылса, құрылғыны қайта іске қоспас немесе өшірмес бұрын жаңартуды орнату орындалады. Әйтпесе, жаңартуларды орнату кесте бойынша жүзеге асырылады.

     Жаңартуларды орнату құрылғылардың жұмысына әсер етуі мүмкін болса, осы жалаушаны қойыңыз.

     Әдепкі бойынша, параметр өшірулі.

   - **Қажетті жалпы жүйелік құрамдастарды орнату**

     Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

     Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

     Әдепкі бойынша, параметр өшірулі.

   - **Жаңартулар кезінде бағдарламаның жаңа нұсқаларын орнатуға рұқсат ету**

     Бұл опция қосылған болса, бағдарламалық жасақтама қолданбасының жаңа нұсқасын орнатуға әкелсе, жаңартуларға рұқсат беріледі.

     Бұл параметр өшірулі болса, бағдарлама жаңартылмайды. Бағдарламалардың жаңа нұсқаларын кейінірек қолмен немесе басқа тапсырманы қолдана отырып, орнатуға болады. Мысалы, егер сіздің компанияңыздың инфрақұрылымы бағдарламаның жаңа нұсқасын қолдамаса немесе сынақ инфрақұрылымындағы жаңартуды тексеру қажет болса, бұл параметрді пайдалануға болады.

     Әдепкі бойынша, параметр қосулы.

     > Бағдарламаның жаңа нұсқасын орнатқаннан кейін, клиент құрылғыларында орнатылған және жаңартылатын бағдарламаның жұмысына байланысты басқа бағдарламалардың жұмысы бұзылуы мүмкін.

   - **Жаңартуларды құрылғыға орнатпастан жүктеп алу**

     Егер жалауша қойылса, бағдарлама жаңартуларды құрылғыға жүктейді, бірақ оларды автоматты түрде орнатпайды. Содан кейін, жүктелген жаңартуларды қолмен орнатуға болады.

     Microsoft жаңартулары Windows қызметтік қалтасына жүктеледі. Үшінші тарап бағдарламаларының жаңартулары (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) **Жаңартуларды келесі жерге жүктеп алу** өрісінде көрсетілген қалтаға жүктеледі.

     Егер бұл параметр өшірулі болса, жаңартулар құрылғыға автоматты түрде орнатылады.

     Әдепкі бойынша, параметр өшірулі.

- **Жаңартуларды келесі жерге жүктеп алу**

  Бұл қалта, үшінші тарап бағдарламаларының (Kaspersky мен Microsoft корпорациясынан басқа өндірушілер шығарған бағдарламалар) жаңартуларын жүктеу үшін қолданылады.

- **Кеңейтілген диагностикалау параметрін қосу**

  Бұл мүмкіндік қосылса, Kaspersky Security Center қашықтан диагностикалау утилитасындағы желілік агент үшін трассирлеу файлдарын жазу өшірулі болса да, желілік агент трассирлеу файлдарын жазады. Трассалау кезекпен екі файлға жазылады; әр файлдың өлшемі **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)** өрісінде көрсетілген мәннің жартысына тең. Екі файл да толтырылған кезде, Желілік агент деректерді үстінен жаза бастайды. Трассалау файлдары %WINDIR%\Temp қалтасында сақталады. Файлдарға қашықтан диагностикалау утилитасы арқылы қатынасуға, сондай-ақ файлдарды жүктеуге немесе жоюға болады.

  Егер бұл функция өшірілген болса, Желілік агент трассалауды Kaspersky Security Center қашықтан диагностикалау утилитасының параметрлеріне сәйкес жазады. Қосымша трассалау жазылмайды.

  Тапсырма жасау кезінде кеңейтілген диагностиканы қосудың қажеті жоқ. Болашақта сізге бұл функцияны пайдалану қажет болуы мүмкін, мысалы, егер қандай да бір құрылғыда тапсырманы іске қосу сәтсіз аяқталса және келесі тапсырманы іске қосу кезінде қосымша ақпарат алу қажет болса.

  Әдепкі бойынша, параметр өшірулі.

- **Кеңейтілген диагностикалау файлдарының ең үлкен өлшемі (МБ)**

  Әдепкі бойынша, 100 МБ мәні және 1-ден 2048 МБ-қа дейінгі рұқсат етілген мәндер көрсетілген. Kaspersky Техникалық қолдау қызметі мамандары, сіз жіберген кеңейтілген диагностика файлдарында мәселені жою үшін жеткілікті ақпарат болмаса, сізден әдепкі бойынша белгіленген мәнді өзгертуді сұрауы мүмкін.

7. Операциялық жүйені қайта іске қосу параметрлерін көрсетіңіз:

- **Құрылғыны қайта іске қоспау**

  Операция аяқталғаннан кейін, клиент құрылғылары автоматты түрде қайта жүктелмейді. Операцияны аяқтау үшін құрылғыны қайта қосу қажет (мысалы, қолмен немесе құрылғыны басқару тапсырмасы арқылы). Қайта жүктеу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа, үздіксіз жұмыс өте маңызды болып саналатын серверлердегі және басқа құрылғылардағы тапсырмалар үшін жарамды.

- **Құрылғыны қайта іске қосу**

  Бұл жағдайда, операцияны аяқтау үшін қайта жүктеу қажет болса, қайта жүктеу әрқашан автоматты түрде орындалады. Бұл нұсқа, мезгіл-мезгіл үзілістерге (өшіру, қайта жүктеу) рұқсат етілген құрылғылардағы тапсырмалар үшін жарамды.

- **Пайдаланушыдан әрекетті орындауды сұрау**

  Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). Бұл нұсқа жұмыс станциялары үшін оңтайлы болып табылады, сондықтан пайдаланушылар қайта жүктеудің ең қолайлы уақытын таңдай алады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **Сұрауды қайталау жиілігі (мин)**

  Егер бұл нұсқа таңдалса, белгілі бір жиіліктегі бағдарлама пайдаланушыға операциялық жүйені қайта жүктеуді ұсынады.

Әдепкі бойынша, параметр қосулы. Әдепкі бойынша аралық 5 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

Егер параметр өшірулі болса, қайта жүктеу ұсынысы тек бір рет көрсетіледі.

- **Келесі уақыттан кейін қайта іске қосу (мин)**

  Пайдаланушыға операциялық жүйені қайта жүктеуді ұсынғаннан кейін, бағдарлама көрсетілген уақыттан кейін мәжбүрлеп қайта жүктеуді орындайды.

  Әдепкі бойынша, параметр қосулы. Әдепкі бойынша уақыт аралығы 30 минутты құрайды. Рұқсат етілген мәндер: 1-ден 1440 минутқа дейін.

- **Бұғатталған сессияларда бағдар. келесі уақыттан кейін мәжбүрлеп жабу (мин)**

  Пайдаланушының құрылғысы бұғатталған кезде бағдарламаларды мәжбүрлеп аяқтау (белсенді емес кезеңнен кейін автоматты түрде немесе қолмен).

  Егер параметр қосулы болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы енгізу өрісінде көрсетілген уақыт өткеннен кейін тоқтатылады.

  Егер параметр өшірулі болса, бұғатталған құрылғыдағы бағдарламалардың жұмысы тоқтамайды.

  Әдепкі бойынша, параметр өшірулі.

8. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** бетінде **Тапсырманы жасауды аяқтау** параметрін қоссаңыз, әдепкі бойынша белгіленген тапсырма параметрлері мәндерін өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

9. **Аяқтау** түймесін басыңыз.

   Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі.

10. Тапсырма сипаттары терезесін ашу үшін жасалған тапсырманың атын басыңыз.

11. Тапсырма сипаттары терезесінде өзіңіздің талаптарыңызға сай тапсырманың жалпы параметрлерін көрсетіңіз.

12. **Сақтау** түймесін басыңыз.

    Тапсырма жасалды және конфигурацияланды.

Тапсырманың нәтижелерінде 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" қатесі туралы ескерту бар болса, бұл мәселені Windows тізімдемесі арқылы шешуге болады.

Жаңартуларды орнату үшін ережелер қосу

Бұл функционалдық, Осалдықтар мен патчтарды басқаруға арналған лицензия болған кезде қолжетімді.

Бағдарламалық жасақтама жаңартуларын орнату немесе *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасын қолдана отырып, бағдарламалардағы осалдықтарды түзету кезінде жаңартуларды орнату ережелерін көрсету қажет. Бұл ережелер орнатылатын жаңартуларды және түзетілетін осалдықтарды анықтайды.

Нақты параметрлер барлық Windows Update жаңартулары үшін немесе үшінші тарап бағдарламалық жасақтамасының жаңартулары үшін ереже қосатыныңызға байланысты (яғни Kaspersky немесе Microsoft шығармаған бағдарламалар). Windows Update жаңартулары немесе үшінші тарап бағдарламаларының жаңартулары үшін ереже қосқанда, жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдауға болады. Барлық жаңартулар үшін ереже қосқанда, сіз орнатылатын жаңартуларды және жаңартуларды орнату арқылы түзетілетін осалдықтарды таңдай аласыз.

Жаңартуларды орнату ережесін келесі жолдармен қосуға болады:

- Қажетті жаңартуларды орнату және осалдықтарды түзету тапсырмасын жасау кезінде ереже қосу.
- **Бағдарлама параметрлері** қойыншасында, тиісті *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмасы сипаттары терезесінде ереже қосу.
- Жаңартуды орнату шебері немесе осалдықтарды түзету шебері көмегімен.

Барлық жаңартуларге ережені қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрі** бетінде **Барлық жаңартуларға арналған ереже** тармағын таңдаңыз.

3. Ашылмалы тізімдегі **Жалпы критерийлер** терезесінде келесі параметрлерді көрсетіңіз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Жаңартулар** терезесінде орнатылатын жаңартуларды таңдаңыз:

   - **Барлық жарамды жаңартуларды орнату**

     Бұл жағдайда, **Жалпы критерийлер** шебері терезесінде көрсетілген өлшемшарттарға сәйкес келетін бағдарламалық жасақтаманың барлық жаңартулары орнатылады. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі жаңартуларды орнату**

     Бұл жағдайда, тізімде қолмен таңдайтын бағдарламалық жасақтаманың жаңартулары ғана орнатылады. Бұл тізімде барлық қолжетімді бағдарламалық жасақтама жаңартулары бар.

     Мысалы, келесі жағдайларда жаңартуларды орнатуға болады: тек критикалық маңызды бағдарламаларды жаңарту үшін немесе тек қажетті бағдарламаларды жаңарту үшін сынақ ортасында жаңартуларды орнатуды тексеру.

     - **Таңдалған жаңартуларды орнату үшін керек бағдарламалардың алдыңғы жаңартуларының барлығын автоматты түрде орнату**

       Таңдалған жаңартуларды орнату үшін, қажет болған жағдайда, бағдарламалардың аралық нұсқаларын орнатуға келіссеңіз, осы параметрді қосыңыз.

       Егер бұл параметр өшірулі болса, бағдарламалардың тек таңдалған нұсқалары орнатылады. Бағдарламалардың нұсқаларын дәйекті түрде орнатуға тырыспай, бағдарламаларды тікелей жаңартқыңыз келсе, бұл параметрді өшіріңіз. Егер таңдалған жаңартуларды бағдарламаның алдыңғы нұсқаларын орнатпай-ақ орнату мүмкін болмаса, бағдарламаны жаңарту қатемен аяқталады.

       Мысалы, сізде құрылғыда бағдарламаның 3-нұсқасы бар, оны 5-нұсқаға жаңартқыңыз келеді, бірақ 5-нұсқаны тек 4-нұсқаның үстіне орнатуға болады. Егер бұл параметр қосулы болса, алдымен бағдарламалық жасақтаманың 4-нұсқасы, содан кейін 5-нұсқасы орнатылады. Егер бұл параметр өшірулі болса, бағдарламалық жасақтаманы жаңарту сәтсіз болады.

       Әдепкі бойынша, параметр қосулы.

5. **Осалдықтар** терезесінде, көрсетілген жаңартуды орнатумен түзетілетін осалдықтарды таңдаңыз:

   - **Қалған критерийлерге сай барлық осалдықтарды жабу**

     Бұл жағдайда, **Жалпы критерийлер** шебері терезесінде көрсетілген өлшемшарттарға сәйкес келетін бағдарламалық жасақтаманың барлық осалдықтары түзетіледі. Әдепкі бойынша таңдалған.

   - **Тек тізімдегі осалдықтарды жабу**

     Тізімнен қолмен таңдалған осалдықтарды ғана түзетіңіз. Бұл тізімде барлық анықталған осалдықтар бар.

     Мысалы, келесі жағдайларда осалдықтарды белгілеуге болады: сынақ ортасындағы осалдықтардың түзетілуін тексеру, тек маңызды бағдарламалардағы осалдықтарды түзету немесе тек қажетті бағдарламалардағы осалдықтарды түзету үшін.

6. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Windows Update жаңартуларына ережені қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрі** бетінде **Windows Update жаңартуларына арналған ереже** тармағын таңдаңыз.

3. **Жалпы шарттар** терезесінде келесі параметрлерді конфигурациялаңыз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

   - **MSRC бойынша қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Microsoft Security Response Center (MSRC) орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Төмен**, **Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Жаңартулардың санаттары** терезесінде орнату үшін жаңарту санаттарын таңдаңыз. Бұл санаттар Microsoft Update каталогымен бірдей. Әдепкі бойынша барлық санаттар таңдалған.

6. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, **Параметрлер** бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Үшінші тарап бағдарламаларын жаңарту ережесін қосу үшін:

1. **Қосу** түймесін басыңыз.

   Ережені жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

2. **Ереже түрі** бетінде **Үшінші тарап жаңартуларға арналған ереже** тармағын таңдаңыз.

3. **Жалпы шарттар** терезесінде келесі параметрлерді конфигурациялаңыз:

   - **Орнатылатын жаңартулар жиынтығы**

     Клиент құрылғыларына орнатылатын жаңартуларды таңдаңыз:

     - **Тек бекітілген жаңартуларды орнату**. Бұл жағдайда, тек расталған жаңартуларды орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартулардан басқа)**. Бұл жағдайда, *Расталды* немесе *Анықталмаған* күйлері бар жаңартулар орнатылады.
     - **Барлық жаңартуларды орнату (қабылданбаған жаңартуларды қоса)**. Бұл жағдайда, барлық жаңартулар олардың растау мәртебесіне қарамастан орнатылады. Бұл нұсқаны мұқият таңдаңыз. Мысалы, сынақ инфрақұрылымында кейбір қабылданбаған жаңартулардың орнатылуын тексергіңіз келсе, осы параметрді пайдаланыңыз.

   - **Қауіптілік деңгейі келесіге тең не одан жоғарырақ осалдықтарды түзету**

     Кейде бағдарламалық жасақтама жаңартуы пайдаланушының бағдарламалық жасақтамамен жұмысын нашарлатуы мүмкін. Мұндай жағдайларда, сіз тек бағдарламалық жасақтама үшін маңызды жаңартуларды орнатып, басқа жаңартуларды өткізіп жібере аласыз.

     Егер бұл параметр қосылса, жаңартулар тек Kaspersky орнатқан критикалық деңгей тізімде таңдалған мәнге тең келетін немесе одан асатын осалдықтарды ғана түзетеді (**Орташа**, **Жоғары**, немесе **Критикалық**). Таңдалған мәннен төмен критикалық деңгейі бар осалдықтар түзетілмейді.

     Егер бұл параметр өшірулі болса, жаңартулар олардың критикалық деңгейіне қарамастан барлық осалдықтарды түзетеді.

     Әдепкі бойынша, параметр өшірулі.

4. **Бағдарламалар** терезесінде жаңартуларды орнатқыңыз келетін бағдарламалар мен бағдарламалардың нұсқаларын таңдаңыз. Әдепкі бойынша барлық бағдарламалар таңдалған.

5. **Атауы** терезесінде қосылатын ереженің атауын көрсетіңіз. Ереже атауын кейінірек, Параметрлер бөлімінде, жасалған тапсырманың сипаттары терезесінде өзгертуге болады.

Ереже жасау шебері өз жұмысын аяқтағаннан кейін, ереже қосылады және тапсырма жасау шеберінің ережелер тізімінде немесе тапсырманың сипаттарында көрсетіледі.

Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушы түзетулері

Осалдықтарды түзету тапсырмасын пайдалану үшін, тапсырма параметрлерінде тізімделген үшінші тарап бағдарламаларындағы осалдықтарды түзету үшін бағдарламалық жасақтама жаңартуларын қолмен көрсету керек. *Осалдықтарды түзету* тапсырмасы Microsoft бағдарламаларының ұсынылған түзетулерін және басқа үшінші тарап бағдарламалары үшін пайдаланушылық түзетулерді пайдаланады. *Пайдаланушылық түзетулер* – бұл әкімші орнату үшін қолмен көрсететін осалдықтарды түзетуге арналған бағдарламалық жасақтама жаңартулары.

Үшінші тарап бағдарламаларындағы осалдықтарға арналған пайдаланушылық түзетулерді таңдау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Беттерде клиент құрылғыларында анықталған бағдарламалардағы осалдықтар тізімі көрсетіледі.

2. Бағдарламалық жасақтама осалдықтары тізімінде пайдаланушылық түзетуді көрсеткіңіз келетін осалдық атауы бар сілтемеге өтіңіз.

   Осалдық сипаттары терезесі ашылады.

3. Сол жақ тақтадан **Пайдаланушылық және басқа түзетулер** бөлімін таңдаңыз.

   Таңдалған бағдарламалық жасақтама осалдықтары үшін пайдаланушылық түзетулердің тізімі көрсетіледі.

4. **Қосу** түймесін басыңыз.

   Қолжетімді орнату пакеттері тізімі көрсетіледі. Көрсетілген орнату пакеттері тізімі **Операциялар → Қоймалар → Орнату пакеттері** қалтасындағы тізімге сай келеді. Егер сіз таңдалған осалдықты түзету үшін пайдаланушылық түзетуді қамтитын орнату пакетін жасамаған болсаңыз, орнату пакетін жасау шеберін іске қосу арқылы пакетті қазір жасауға болады.

5. Үшінші тарап бағдарламаларының осалдығы үшін пайдаланушылық түзетуді (немесе пайдаланушылық түзетулерді) қамтитын орнату пакетін (немесе пакеттерін) таңдаңыз.

6. **Сақтау** түймесін басыңыз.

Бағдарламалық жасақтама осалдықтарына арналған пайдаланушылық түзетулерді қамтитын орнату пакеттері көрсетілген. *Осалдықтарды түзету* тапсырмасын іске қосқаннан кейін, орнату пакеті орнатылып, бағдарламалық жасақтама осалдықтары жабылады.

Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау

Басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтардың бар-жоғы тұрғысынан тексерілгеннен кейін, сіз барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар тізімін қарап шыға аласыз. Басқару сервері иерархиясы үшін тапсырманы іске қоссаңыз, осалдықтары анықталған басқарылатын құрылғылар тізімін тек таңдалған Басқару сервері үшін көре аласыз.

Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар тізімін қарау үшін,

Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

Беттерде клиент құрылғыларында анықталған бағдарламалардағы осалдықтар тізімі көрсетіледі.

Сондай-ақ, осалдықтар туралы есепті жасауға және көруге болады.

Бағдарламалардағы осалдықтар тізімін қарау үшін сүзгіні көрсете аласыз. Сүзгіні басқару үшін бағдарламалардағы осалдықтар тізімінің жоғарғы оң жақ бұрышындағы **Сүзгі** () белгішесін басыңыз. Сонымен қатар, бағдарламалық жасақтама осалдықтары тізімінің үстіндегі **Алдын ала орнатылған сүзгілер** ашылмалы тізімінде алдын ала орнатылған сүзгілердің бірін таңдай аласыз.

Тізімдегі кез келген осалдық туралы толық ақпаратты ала аласыз.

Бағдарламалық жасақтама осалдықтары туралы ақпаратты алу үшін,

бағдарламалық жасақтама осалдықтары тізімінде осалдықтың атауы көрсетілген сілтемеден өтіңіз.

Бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

Таңдалған басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар туралы ақпаратты қарау

Сіз осалдықтар туралы ақпаратты таңдалған Windows басқарылатын құрылғысында табылған бағдарламалардан көре аласыз.

Таңдалған басқарылатын құрылғыда анықталған бағдарламалық жасақтама осалдықтары тізімін көру үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде, бағдарламаларда анықталған осалдықтарды көргіңіз келетін құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. Таңдалған құрылғы сипаттары терезесінде **Кеңейтілген** қойындысын таңдаңыз.

4. Сол жақ тақтадан **Бағдарламалық жасақтама осалдықтары** бөлімін таңдаңыз.

Таңдалған басқарылатын құрылғыда табылған бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

Таңдалған бағдарламалық жасақтама осалдықтары сипаттарын көру үшін,

бағдарламалардағы осалдықтар тізіміндегі осалдық атауы бар сілтемеге өтіңіз.

Таңдалған бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

Басқарылатын құрылғылардағы осалдықтардың статистикасын қарау

Басқарылатын құрылғылардағы бағдарламалардағы әрбір осалдықтың статистикалық ақпаратын көруге болады. Статистика диаграммалар түрінде ұсынылған. Диаграмма келесі күйлері бар құрылғылардың санын көрсетеді:

- *Еленбеген: <құрылғылар саны>*. Егер сіз осалдық сипаттарында осалдықты елемеу параметрін қолмен орнатсаңыз, осы күй тағайындалады.
- *Түзетілген: <құрылғылар саны>*. Егер осалдықты түзету тапсырмасы сәтті аяқталса, осы күй белгіленеді.
- *Түзетуге жоспарланған: <құрылғылар саны>* Егер сіз осалдықтарды түзету тапсырмасын жасаған болсаңыз, бірақ тапсырма әлі аяқталмаған болса, осы күй белгіленеді.

- *Патч қолданылған: <құрылғылардың саны>*. Егер сіз осалдықты түзету үшін бағдарламалық жасақтаманы жаңартуды қолмен таңдаған болсаңыз, осы күй тағайындалады, бірақ бұл жаңарту осалдықты түзетпеді.

- *Түзету қажет: <құрылғылар саны>*. Осалдық кейбір басқарылатын құрылғыларда ғана жабылған болса, бірақ басқа басқарылатын құрылғыларда осалдықты түзету қажет болса, осы күй тағайындалады.

Басқарылатын құрылғылардағы осалдық статистикасын көру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда табылған бағдарламалардағы осалдықтар тізімі бар бет көрсетіледі.

2. Қажетті осалдықтың жанына жалаушаны қойыңыз.

3. **Құрылғылардағы осалдық статистикасы** түймесін басыңыз.

Осалдық күйінің диаграммасы көрсетіледі. Күйді басу арқылы, осалдықтың таңдалған күйі бар құрылғылардың тізімі ашылады.

Бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау

Көрсетілген осалдықтар тізімін CSV немесе TXT пішіміндегі файлға экспорттауға болады. Сіз бұл файлдарды, мысалы, ақпараттық қауіпсіздік жөніндегі басшыңызға жіберу немесе статистика мақсатында сақтау үшін пайдалана аласыз.

Барлық басқарылатын құрылғыларда анықталған бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Басқарылатын құрылғыларда табылған бағдарламалардағы осалдықтар тізімі бар бет көрсетіледі.

2. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз.

Бағдарламалық жасақтама осалдықтары тізімін қамтитын файл, қазіргі сәтте қолданылып жатқан құрылғыға жүктеледі.

Таңдалған басқарылатын құрылғыларда табылған бағдарламалардағы осалдықтар тізімін мәтіндік файлға экспорттау үшін:

1. Таңдалған басқарылатын құрылғыда табылған бағдарламалық жасақтама осалдықтары тізімін ашыңыз.

2. Экспорттағыңыз келетін бағдарламалық жасақтама осалдықтарын таңдаңыз.

   Басқарылатын құрылғыларда табылған бағдарламалардағы осалдықтардың толық тізімін экспорттағыңыз келсе, бұл қадамды өткізіп жіберіңіз.

Басқарылатын құрылғыда табылған бағдарламалардағы осалдықтардың толық тізімін экспорттау кезінде тек ағымдағы бетте көрсетілген осалдықтар экспортталады.

3. Экспорттағыңыз келетін пішімге байланысты, **TXT файлына экспорттау** немесе **CSV файлына экспорттау** түймесін басыңыз.

Бағдарламалық жасақтама осалдықтары тізімін қамтитын файл, қазіргі сәтте қолданылып жатқан таңдалған басқарылатын құрылғыдан экспортталады.

Бағдарламалардағы осалдықтарды елемеу

Бағдарламалық жасақтама осалдықтарын елемеуіңіз және оларды түзетпеуіңіз мүмкін. Бағдарламалардағы осалдықтарды елемеу себептері, мысалы, келесідей болуы мүмкін:

- Сіз бағдарламадағы осалдықты ұйымыңыз үшін критикалық деп санамайсыз.
- Бағдарламалық жасақтама осалдықтарын түзету, осалдықты түзетуді қажет ететін бағдарламаның деректерін зақымдауы мүмкін екенін түсінесіз.
- Бағдарламалық жасақтама осалдықтары сіздің ұйымыңыздың желісіне қауіп төндірмейтініне сенімдісіз, өйткені сіз басқарылатын құрылғыларды қорғау үшін басқа шараларды қолданасыз.

Барлық басқарылатын құрылғылардағы немесе тек таңдалған басқарылатын құрылғылардағы бағдарламалардағы осалдықты елемеуге болады.

Барлық басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын өткізіп жіберу үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Патчтарды басқару → Бағдарламалық жасақтама осалдықтары** бөліміне өтіңіз.

   Бетте басқарылатын құрылғыларда табылған бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

2. Бағдарламалық жасақтама осалдықтары тізімінде өткізіп жібергіңіз келетін бағдарламалық жасақтама осалдықтары атауын басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

3. **Жалпы** қойындысында **Осалдықты елемеу** параметрін қосыңыз.

4. **Сақтау** түймесін басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі жабылады.

Бағдарламалық жасақтама осалдықтары барлық басқарылатын құрылғыларда өткізіп жіберіледі.

Таңдалған басқарылатын құрылғылардағы бағдарламалық жасақтама осалдықтарын өткізіп жіберу үшін:

1. Негізгі мәзірде **Активтер (құрылғылар) → Басқарылатын құрылғылар** тармағына өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде бағдарламалық жасақтама осалдықтарын жіберіп алғыңыз келетін құрылғы атауымен сілтемеге өтіңіз.

   Құрылғы сипаттары терезесі ашылады.

3. Құрылғы сипаттары терезесінде **Кеңейтілген** бөлімін таңдаңыз.

4. Сол жақ тақтадан **Бағдарламалық жасақтама осалдықтары** бөлімін таңдаңыз.

   Құрылғыда табылған бағдарламалық жасақтама осалдықтары тізімі көрсетіледі.

5. Бағдарламалық жасақтама осалдықтары тізімінен таңдалған құрылғыда өткізіп жібергіңіз келетін осалдықты таңдаңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі ашылады.

6. Бағдарламалық жасақтама осалдықтары сипаттары терезесінде, **Жалпы** қойындысында **Осалдықты елемеу** параметрін қосыңыз.

7. **Сақтау** түймесін басыңыз.

   Бағдарламалық жасақтама осалдықтары сипаттары терезесі жабылады.

8. Құрылғының сипаттар терезесін жабыңыз.

Бағдарламалық жасақтама осалдықтары таңдалған құрылғыда өткізіп жіберіледі.

Өткізіп жіберілген бағдарламалық жасақтама осалдықтары *Осалдықтарды түзету* және *Қажетті жаңартуларды орнату және осалдықтарды түзету* тапсырмаларының жұмысы аяқталғаннан кейін жабылмайды. Бағдарламалардағы жетіспейтін осалдықтарды осалдықтар тізімінен сүзгі арқылы алып тастауға болады.

Клиент құрылғыларында бағдарламалардың іске қосылуын басқару

Бұл бөлімде клиент құрылғыларында іске қосылған бағдарламаларды басқарумен байланысты Kaspersky Security Center мүмкіндіктері сипатталған.

Орындалатын файлдарды басқару үшін Бағдарламаларды басқару компонентін пайдалану

Пайдаланушы құрылғыларында орындалатын файлдардың орындалуына рұқсат беру немесе тыйым салу үшін Бағдарламаларды бақылау компонентін пайдалануға болады. Бағдарламаларды бақылау компоненті Windows және Linux операциялық жүйелерін қолдайды.

Linux негізіндегі операциялық жүйелер үшін қолданбаларды басқару құрамдасы Linux-ке арналған Kaspersky Endpoint Security 11.2 нұсқасынан бастап қолжетімді. Сондай-ақ құрамдас Windows 3.0 немесе одан кейінгі нұсқасына арналған Kaspersky Embedded Systems Security үшін қолжетімді.

Алдын ала талаптар

- Kaspersky Security Center бағдарламасы сіздің ұйымыңызда орналастырылған.
- Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Linux саясаты жасалды және белсенді.
- Kaspersky Embedded Systems Security for Windows немесе Kaspersky Embedded Systems Security for Linux саясаты жасалды және белсенді.

Кезеңдер

Бағдарламаны басқару құрамдасын қолдану сценарийі келесі кезеңдерден тұрады:

1. **Клиент құрылғыларында орындалатын файлдар тізімін құрастыру және қарау**

   Бұл кезең сізге басқарылатын құрылғыларда қандай орындалатын файлдардың орнатылғанын анықтауға көмектеседі. Орындалатын файлдар тізімін қарап шығыңыз және оны рұқсат етілген және тыйым салынған орындалатын файлдардың тізімдерімен салыстырыңыз. Орындалатын файлдарды қолданудағы шектеулер ұйымдағы ақпараттық қауіпсіздік саясаттарымен байланысты болуы мүмкін.

   Нұсқаулар:

   - Басқару консолі: Орындалатын файлдарды түгендеу.
   - Kaspersky Security Center Web Console: Клиент құрылғыларында сақталатын орындалатын файлдар тізімін алу және қарау.

2. **Ұйымыңызда қолданылатын орындалатын файлдар үшін санаттарды жасау**

   Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімдерін талдаңыз. Талдау негізінде орындалатын файлдар үшін санаттарды қалыптастырыңыз. Ұйымыңызда қолданылатын орындалатын файлдардың стандартты жиынтығын қамтитын "Жұмыс бағдарламалары" санатын құру ұсынылады. Егер әртүрлі қауіпсіздік топтары өз жұмысында өзіндік орындалатын файлдар жиынтығын қолданса, әр қауіпсіздік тобы үшін бөлек санатты құруға болады.

   Нұсқаулар:

   - Басқару консолі: Қолмен толықтырылатын бағдарламалар санатын құру, Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын құру, Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру.
   - Kaspersky Security Center Web Console: Қолмен толықтырылатын бағдарламалар санатын құру, Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын құру, Көрсетілген қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру.

3. **Kaspersky Endpoint Security саясатындағы Бағдарламаларды басқару конфигурациялау**

   Алдыңғы кезеңде жасаған санаттарды қолдана отырып, Kaspersky Endpoint Security саясатындағы Бағдарламаларды басқару құрамдасын конфигурациялаңыз.

Нұсқаулар:

- Басқару консолі: Клиент құрылғыларында бағдарламаларды іске қосуды басқаруды конфигурациялау.
- Kaspersky Security Center Web Console: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау.

4. **Kaspersky Embedded Systems Security қолданба саясатындағы қолданбаларды басқаруды конфигурациялау**

   Жасалған санаттарды пайдалану арқылы Kaspersky Embedded Systems Security for Windows саясатындағы қолданбаларды басқару құрамдасын конфигурациялаңыз. Қолданбаларды басқару құрамдасы туралы қосымша ақпарат алу үшін Kaspersky Embedded Systems Security for Windows Help немесе Kaspersky Embedded Systems Security for Linux анықтамасын қараңыз.

   Ережелердің көп санын пайдалансаңыз, саясатты жүктеу кезінде қате орын алуы мүмкін. Келесі пәрмендерді пайдалану байт өлшеміндегі максималды сұрау өлшемін арттыруға болады:

   - JSON сұрауы үшін:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

   - HTTP сұрауы үшін:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
     ```

     Бұл жерде `<max_request_size>` — байт өлшеміндегі максималды сұрау өлшемі (мысалы, `200000000`).

5. **Тест режимінде Бағдарламаларды басқару құрамдасын қосу**

   Бағдарламаларды басқару ережелері пайдаланушылардың жұмысына қажетті орындалатын файлдарды бұғаттамауы үшін, Қолданбаларды бақылау ережелерін тестілеуді қосып, ережелер жасалғаннан кейін олардың жұмысын талдау ұсынылады. Сынау қосылған кезде, Kaspersky Endpoint Security for Windows немесе Kaspersky Embedded Systems Security саясаты қолданбаларды басқару ережелері іске қосуды тыйым салынған орындалатын файлдарды бұғаттамайды, бірақ оның орнына басқару серверіне олардың іске қосылуы туралы хабарландырулар жібереді.

   Бағдарламаларды бақылау ережелерін тестілеу кезінде келесі әрекеттерді орындау ұсынылады:

   - Тестілеу кезеңін анықтаңыз. Тестілеу кезеңі бірнеше күннен екі айға дейін өзгеруі мүмкін.
   - Бағдарламаны басқару құрамдасының жұмысын тексеру нәтижесінде пайда болатын оқиғаларды зерттеңіз.

   Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындаңыз және орнату процесінде **Сынақ режимі** опциясын қосыңыз.

6. **Бағдарламаны басқару құрамдасының санаттары параметрлерін өзгерту**

   Қажет болса, Бағдарламаларды басқару құрамдасының параметрлерін өзгертіңіз. Тестілеу нәтижелеріне сүйене отырып, Бағдарламаларды басқару құрамдасының оқиғаларына байланысты орындалатын файлдарды қолмен толықтырылатын санатқа қосуға болады.

   Нұсқаулар:

   - Басқару консолі: Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу.
   - Kaspersky Security Center Web Console: Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу.

7. **Жұмыс режимінде Бағдарламаларды бақылау ережелерін қолдану**

   Бағдарламаларды бақылау ережелерін тексергеннен кейін және санаттарды конфигурациялауды аяқтағаннан кейін, сіз жұмыс режимінде Бағдарламаларды басқару ережелерін қолдана аласыз.

   Kaspersky Security Center Web Console үшін нұсқаулар: Kaspersky Endpoint Security for Windows саясатында Бағдарламаны басқару құрамдасын конфигурациялау. Осы нұсқаулықты орындап, конфигурациялау барысында **Сынақ режимі** параметрін өшіріңіз.

8. **Бағдарламаны басқару конфигурациясын тексеру**

   Келесіні орындағаныңызға көз жеткізіңіз:

   - Орындалатын файлдар үшін санаттар жасадық.
   - Санаттарды қолдана отырып, Бағдарлама санаттарын конфигурацияладыңыз.
   - Жұмыс режимінде Бағдарламаларды бақылау ережелерін қолдандыңыз.

Нәтижелер

Сценарий аяқталғаннан кейін, басқарылатын құрылғыларда орындалатын файлдардың іске қосылуы бақыланады. Пайдаланушылар сіздің ұйымыңызда рұқсат етілген орындалатын файлдарды ғана басқара алады және сіздің ұйымыңызда тыйым салынған орындалатын файлдарды іске қоса алмайды.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Қолданбаны басқару компонентінің режимдері мен категориялары

Қолданбаны бақылау компоненті пайдаланушының бағдарламаларды іске қосу әрекеттерін бақылайды. Бағдарламаларды іске қосуды басқару үшін Қолданбаны басқару компонентінің ережелерін пайдалануға болады.

Қолданбаларды басқару құрамдас бөлігі Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security 11.2 for Linux және одан да жоғары нұсқалар, Kaspersky Security for Virtualization Жеңіл агент үшін қолжетімді. Бұл бөлімдегі барлық нұсқаулар Kaspersky Endpoint Security for Windows бағдарламасына арналған Бағдарламаны басқару конфигурациясын сипаттайды.

Бағдарламаларды бақылау ережесінің ешқайсысына сәйкес келмейтін параметрлері бар орындалатын файлдарды іске қосу, келесі құрамдастың таңдалған жұмыс режимі тарапынан реттеледі:

- *Тыйым салу тізімі*. Егер сіз тыйым салу ережелерінде көрсетілгендерден басқа барлық орындалатын файлдардың іске қосылуына рұқсат бергіңіз келсе, режим қолданылады. Әдепкі бойынша осы режим таңдалған.

- *Рұқсат ету тізімі*. Рұқсат ету ережелерінде көрсетілгендерден басқа барлық орындалатын файлдарды іске қосуға тыйым салғыңыз келсе, режим пайдаланылады.

Бағдарламаларды бақылау ережелері орындалатын файлдар санаттарында жүзеге асырылған. Kaspersky Security Center бағдарламасында санаттардың үш түрі бар:

- Қолмен толтырылатын санат. Сіз орындалатын файлдарды санатқа қосу үшін файл метадеректері, файл хэші, файл сертификаты, KL санаты, файл жолы сияқты шарттарды анықтайсыз.

- Таңдалған құрылғылардағы орындалатын файлдар кіретін санат. Сіз орындалатын файлдары автоматты түрде санатқа қосылатын құрылғыны көрсетесіз.

- Таңдалған қалталардан алынған орындалатын файлдарды қамтитын санат. Сіз орындалатын файлдар автоматты түрде санатқа кіретін қалтаны көрсетесіз.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу және қарау

Клиент құрылғыларында сақталған орындалатын файлдар тізімін келесі жолдардың бірімен алуға болады:

- Kaspersky Endpoint Security саясатында қолданбаларды іске қосу туралы хабарландыруларды қосу.

- Түгендеу тапсырмасын жасау.

Kaspersky Endpoint Security саясатында қолданбаларды іске қосу туралы хабарландыруларды қосу

Бағдарламаларды іске қосу туралы хабарландыруларды қосу үшін:

1. Kaspersky Endpoint Security саясат параметрлерін ашыңыз, содан кейін **Жалпы параметрлер** → **Есептер және қоймалар** тармағына өтіңіз.

2. **Деректерді әкімші серверіне тасымалдау** параметрлер тобында **Іске қосылған қолданбалар туралы ақпарат** құсбелгісін қойып, өзгерістерді сақтаңыз.

Пайдаланушы орындалатын файлдарды іске қосуға әрекет жасағанда, осы файлдар туралы ақпарат клиент құрылғысындағы орындалатын файлдар тізіміне қосылады. Kaspersky Endpoint Security бұл ақпаратты желілік агентке жібереді, содан кейін желілік агент оны басқару серверіне жібереді.

Түгендеу тапсырмасын жасау

Орындалатын файлдарды түгендеу функциясы келесі бағдарламалар үшін қолжетімді:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 11.2 және одан жоғары нұсқалары
- Kaspersky Security for Virtualization 4.0 Light Agent және одан да жоғары

Орнатылған бағдарламалар туралы ақпаратты алу арқылы дерекқорға түсетін жүктемені азайтуға болады. Дерекқор орнын үнемдеу үшін бағдарламалық жасақтаманың стандартты жиынтығы орнатылған анықтамалық құрылғыларда түгендеу тапсырмасын іске қосыңыз. Құрылғылардың саны 1-3 болғаны дұрыс.

Төмендегі дерекқорларды пайдаланған кезде түгендеу тапсырмасын орындамаған жөн: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (барлық шығарылым).

Клиент құрылғыларында орындалатын файлдарды түгендеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

   Тапсырмалар тізімі көрсетіледі.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Содан кейін, шебердің нұсқауларын орындаңыз.

3. **Жаңа тапсырма параметрлері** бетінде, **Бағдарлама** ашылмалы тізімінде, клиент құрылғыларының операциялық жүйесінің түріне байланысты Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Linux таңдаңыз.

4. **Тапсырма түрі** ашылмалы тізімінен **Қойма** тармағын таңдаңыз.

5. **Тапсырманы жасауды аяқтау** бетінде **Аяқтау** түймесін басыңыз.

Жаңа тапсырма жасау шебері өз жұмысын аяқтағаннан кейін, **Қойма** тапсырмасы жасалды және конфигурацияланды. Сіз жасалған тапсырманың параметрлерін өзгерте аласыз. Нәтижесінде, жасалған тапсырма тапсырмалар тізімінде көрсетіледі.

Түгендеу тапсырмасының толық сипаттамасын келесі анықтамалардан қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент

Қойма тапсырмасын орындағаннан кейін, басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімі жасалады және сіз осы тізімді қарай аласыз.

Түгендеу кезінде келесі форматтағы орындалатын файлдарды анықтауға болады (түгендеу тапсырмасы сипаттарында таңдалған опцияға байланысты): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

Басқарылатын құрылғыларда сақталған орындалатын файлдардың тізімін көру.

Клиент құрылғыларында сақталатын орындалатын файлдар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Орындалатын файлдар** бөліміне өтіңіз.

Бетте клиент құрылғыларында сақталған орындалатын файлдардың тізімі көрсетіледі.

Қажет болса, басқарылатын құрылғының орындалатын файлын Kaspersky Security Center Web Console ашық құрылғыға жіберуге болады.

Орындалатын файлды жіберу үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Орындалатын файлдар** бөліміне өтіңіз.
2. Жібергіңіз келетін орындалатын файл сілтемесін басыңыз.
3. Ашылған терезеде **Құрылғылар** бөліміне өтіп, орындалатын файлды жібергіңіз келетін басқарылатын құрылғының жанына жалаушаны қойыңыз.

   Орындалатын файлды жібермей тұрып, **Басқару серверімен байланысты үзбеу** құсбелгі ұяшығын таңдап, басқарылатын құрылғыда басқару серверіне тікелей қосылым бар екенін тексеріңіз.

4. **Жіберу** түймесін басыңыз.

   Таңдалған орындалатын файл Kaspersky Security Center Web Console ашық құрылғыға одан әрі жіберу үшін жүктеп алынады.

Қолмен қосылған мазмұнмен қолданба санатын жасау

Сіз өзіңіздің ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдарға арналған үлгі ретінде критерийлер жиынтығын көрсете аласыз. Критерийлерге сәйкес орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасының конфигурациясында қолдана аласыз.

Қолмен толықтырылатын бағдарламалар санатын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Бағдарлама санаттары тізімі бар бет ашылады.

2. **Қосу** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Санатты жасау әдісін таңдау** қадамында **Қолмен қосылған мазмұны бар санат. Орындалатын файлдардың деректері санатқа қолмен қосылады** параметрін таңдаңыз.

4. **Шарттар** қадамында, файлдарды жасалып жатқан санатқа қосуға арналған критерийді қосу үшін **Қосу** түймесін басыңыз.

5. **Жағдай шарттары** қадамында, келесі тізімдегі санатты жасау үшін ереже түрін таңдаңыз:

   - **KL санатынан**

     Осы нұсқа таңдалған болса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде Kaspersky бағдарламалары санатын қосуға болады. Көрсетілген KL санатына кіретін бағдарламалар бағдарламалардың пайдаланушы санатына қосылатын болады.

   - **Репозиторийден сертификатты таңдау**

     Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Санат шарты көрсетілген сертификатпен қол қойылған орындалатын файлдарға ғана сәйкес келеді.

     Түгендеу тапсырмасын жасап, іске қоссаңыз немесе Kaspersky Endpoint Security саясатында **Іске қосылған қолданбалар** туралы құсбелгісін таңдасаңыз, сертификаттар қоймаға қосылады. Сіз екі әрекетті де орындай аласыз.

     > Сертификаттар туралы ақпаратты тек PE форматындағы (.exe, .dll, .sys) орындалатын файлдардан алуға болады.

   - **Қолданба жолын көрсету (қолдау көрсетілетін маскалар)**

     Осы нұсқа таңдалса, орындалатын файлдары бағдарламалардың пайдаланушы санаттарына қосылатын клиент құрылғысындағы файлды немесе қалтаны көрсетуге болады. *C:\path_to_exe** сияқты тұрақты өрнектерді пайдалануға болады, мысалы: *C:\Program Files\Internet Explorer**.

   - **Алынбалы жетек**

     Осы нұсқа таңдалған болса, бағдарлама іске қосылатын тасушының түрін (кез келген немесе алынбалы диск) көрсетуге болады. Таңдалған типтегі тасушыда іске қосылатын бағдарламалар бағдарламалардың пайдаланушы санатына қосылады.

   - **Хэш, метадеректер немесе сертификат**:

     - **Орындалатын файлдар тізімінен таңдау**

       Осы нұсқа таңдалған болса, санатқа қосылатын бағдарламаларды клиент құрылғысындағы орындалатын файлдар тізімінен таңдауға болады.

- **Бағдарламалар тізімдемесінен таңдау**

  Егер бұл параметр таңдалса, бағдарламалар тізімдемесі көрсетіледі. Тізілімнен қолданбаны таңдағаннан кейін сіз таңдаған қолданбаның метадеректерімен толтырылған параметрлермен терезе ашылады:

  - Файл атауы.
  - Файл нұсқасы. Сіз нұсқаның нақты мәнін көрсете аласыз немесе "5.0-ден артық" сияқты шарт жаза аласыз.
  - Бағдарлама атауы.
  - Бағдарлама нұсқасы. Сіз нұсқаның нақты мәнін көрсете аласыз немесе "5.0-ден артық" сияқты шарт жаза аласыз.
  - Өндіруші.

  Сіз таңдаған қолданбаны іске қосу емес, тек көрсетілген параметрлерге сәйкес келетін орындалатын файлдарды іске қосу бұғатталатынын ескеріңіз. Таңдалған қолданба метадеректері қолданбаны іске қосқан кезде іске қосылатын орындалатын файлдың біріне сәйкес келсе, келесі қадамға өтуіңізге болады. Сәйкес келмесе, орындалатын файлдың метадеректеріне сәйкестендіру үшін мәндерді қолмен өзгерту керек.

- **Қолмен көрсету**

  Егер бұл нұсқа таңдалса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде файл хэшін, метадеректерді немесе сертификатты көрсету керек.

  Файл хэші

  Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

  SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы SHA256 хеш функциясын есептеп шығаруды қолдайды. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен нұсқалар үшін қолдау көрсетіледі.

Санат файлдары үшін Kaspersky Security Center бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

- Желіңізде орнатылған қауіпсіздік бағдарламаларының барлық даналары Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы болса, онда **SHA256** жалаушасын қойыңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен бағдарлама нұсқалары үшін, орындалатын файлдың SHA256 өлшемшарты бойынша жасалған санатты қосу ұсынылмайды. Бұл қауіпсіздік бағдарламаның істен шығуына әкелуі мүмкін. Бұл жағдайда, санат файлдары үшін MD5 криптографиялық хеш функциясын қолдана аласыз.

- Сіздің желіңізде Kaspersky Endpoint Security 10 Service Pack 2 for Windows бағдарламасының ең ерте нұсқалары орнатылған болса, **MD5 хэші** тармағын таңдаңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқалары үшін орындалатын файлдың MD5 бақылау сомасының өлшемшарты бойынша жасалған санатты қосуға болмайды. Бұл жағдайда, санат файлдары үшін SHA256 криптографиялық хеш функциясын қолдана аласыз.

- Желіңіздегі әртүрлі құрылғылар Kaspersky Endpoint Security 10 бағдарламасының ең ерте нұсқаларын да, ең кейінгі нұсқаларын да қолданса, онда **SHA256** жалаушасы мен **MD5 хэші** жалаушасын қойыңыз.

Метадеректер

Егер бұл параметр таңдалса, сіз файл атауы, файл нұсқасы және өндіруші сияқты файл метадеректерін көрсете аласыз. Санат шарты тек метадеректері бірдей орындалатын файлдарға сәйкес келеді.

Сертификат

Осы нұсқа таңдалған болса, қоймадағы сертификаттарды көрсетуге болады. Санат шарты көрсетілген сертификатпен қол қойылған орындалатын файлдарға ғана сәйкес келеді.

Түгендеу тапсырмасын жасап, іске қоссаңыз немесе Kaspersky Endpoint Security саясатында **Іске қосылған қолданбалар** туралы құсбелгісін таңдасаңыз, сертификаттар қоймаға қосылады. Сіз екі әрекетті де орындай аласыз.

- **Файлдан немесе MSI пакетінен/мұрағатталған қалтадан**

  Осы нұсқа таңдалған болса, бағдарламаларды пайдаланушы санатына қосу шарты ретінде MSI орнатушы файлын көрсетуге болады. Бағдарлама орнатушының метадеректері Басқару серверіне жіберілетін болады. Орнатушының метадеректері көрсетілген MSI орнатушысына сай келетін қолданбалар қолданбалардың пайдаланушы санатына қосылатын болады.

Таңдалған критерий шарттар тізіміне қосылды.

Бағдарлама санатын жасау үшін қанша критерий қосуға болады.

6. **Ерекшеліктер** қадамында, ерекшеліктер аймағына критерий қосу және файлдарды жасалып жатқан санаттан шығару үшін **Қосу** түймесін басыңыз.

7. **Жағдай шарттары** қадамында, санатты жасау үшін ереже түрін таңдағаныңыздай, тізімнен ереже түрін таңдаңыз.

Шебер аяқталғаннан кейін, бағдарламалар санаты құрылады. Ол бағдарлама санаттарының тізімінде пайда болады. Бағдарламаны басқару құрамдасын конфигурациялау кезінде бағдарламалар санатын жасауға болады.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Таңдалған құрылғылардан орындалатын файлдарды қамтитын бағдарламалар санатын жасау

Құрылғыдан орындалатын файлдарды, іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдардың үлгісі ретінде пайдалануға болады. Таңдалған құрылғылардағы орындалатын файлдардың негізінде, сіз санатты құра аласыз және оны Бағдарламаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Құрылғылардан орындалатын файлдар тізімін алу үшін:

1. Kaspersky Endpoint Security for Windows немесе Kaspersky Endpoint Security for Linux саясаты жасалды және белсенді екеніне көз жеткізіңіз. Саясатта Қолданбаны басқару құрамдас бөлігін қосыңыз.
2. Клиент құрылғыларында сақталған орындалатын файлдардың тізімін алу.

Таңдалған құрылғылардан орындалатын файлдарды қамтитын санатты құру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Санаттар тізімі бар бет ашылады.

2. **Қосу** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Санатты жасау әдісін таңдау** қадамында санат атауын көрсетіп, **Таңдалған құрылғылардағы орындалатын файлдарды қамтитын санат. Осы орындалатын файлдар автоматты түрде өңделеді және метрикалары санатқа қосылады** параметрін таңдаңыз.
4. **Қосу** түймесін басыңыз.
5. Ашылған терезеде санатты құру үшін орындалатын файлдары пайдаланылатын құрылғыны немесе құрылғыларды таңдаңыз.
6. Келесі параметрлерді белгілеңіз:

   - **Хеш функциясын есептеп шығару алгоритмі**

     Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы SHA256 хеш функциясын есептеп шығаруды қолдайды. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен нұсқалар үшін қолдау көрсетіледі.

Санат файлдары үшін Kaspersky Security Center бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

- Желіңізде орнатылған қауіпсіздік бағдарламаларының барлық даналары Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы болса, онда **SHA256** жалаушасын қойыңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен бағдарлама нұсқалары үшін, орындалатын файлдың SHA256 өлшемшарты бойынша жасалған санатты қосу ұсынылмайды. Бұл қауіпсіздік бағдарламаның істен шығуына әкелуі мүмкін. Бұл жағдайда, санат файлдары үшін MD5 криптографиялық хеш функциясын қолдана аласыз.

- Сіздің желіңізде Kaspersky Endpoint Security 10 Service Pack 2 for Windows бағдарламасының ең ерте нұсқалары орнатылған болса, **MD5 хэші** тармағын таңдаңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқалары үшін орындалатын файлдың MD5 бақылау сомасының өлшемшарты бойынша жасалған санатты қосуға болмайды. Бұл жағдайда, санат файлдары үшін SHA256 криптографиялық хеш функциясын қолдана аласыз.

Желіңіздегі әртүрлі құрылғылар Kaspersky Endpoint Security 10 бағдарламасының ең ерте нұсқаларын да, ең кейінгі нұсқаларын да қолданса, онда **SHA256** жалаушасы мен **MD5 хэші** жалаушасын қойыңыз.

Әдепкі бойынша, **Санаттағы файлдар үшін SHA256 есептеп шығару (Kaspersky Endpoint Security 10 Service Pack 2 for Windows үшін қолдау көрсетіледі)** жалаушасы қойылған.

Әдепкі бойынша, **Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)** алынып тасталған.

- **Басқару серверінің қоймасымен деректерді синхрондау**

  Басқару сервері көрсетілген қалтада (немесе қалталарда) өзгерістерді мезгіл-мезгіл тексеріп отыруын қаласаңыз, осы параметрді таңдаңыз.

  Әдепкі бойынша, параметр өшірулі.

  Егер сіз осы параметрді қоссаңыз, көрсетілген қалтада (қалталарда) өзгерістерді тексеру үшін кезеңді (сағатпен) көрсетіңіз. Әдепкі бойынша, тексеру кезеңі 24 сағатқа тең келеді.

- **Файл түрі**

  Бұл бөлімде бағдарламалар санатын құру үшін қолданылатын файл түрін көрсетуге болады.

  Барлық файлдар. Жасалып жатқан санат үшін барлық файлдар ескеріледі. Әдепкі бойынша, осы нұсқа таңдалған.

  Тек бағдарлама санаттарынан тыс файлдар. Құрылған санат үшін тек бағдарлама санаттарынан тыс файлдар ескеріледі.

- **Қалталар**

  Бұл бөлімде бағдарламалар санатын құру үшін пайдаланылатын файлдары бар таңдалған құрылғылардың қалталарын көрсетуге болады.

  Барлық қалталар. Жасалып жатқан санат үшін барлық қалталар ескеріледі. Әдепкі бойынша, осы нұсқа таңдалған.

  Көрсетілген қалта. Жасалып жатқан санат үшін тек көрсетілген қалта ескеріледі. Егер сіз осы параметрді таңдасаңыз, қалта жолын көрсетуіңіз керек.

Шебердің жұмысы аяқталған кезде орындалатын файлдардың санаты жасалады. Ол санаттар тізімінде

пайда болады. Бағдарламаны басқару құрамдасын конфигурациялау кезінде санатты жасауға болады.

Таңдалған қалталардан орындалатын файлдарды қамтитын бағдарламалар санатын құру

Таңдалған қалталардың орындалатын файлдарын, ұйымыңызда іске қосуға рұқсат бергіңіз немесе тыйым салғыңыз келетін орындалатын файлдардың эталондық жиынтығы ретінде пайдалануға болады. Таңдалған қалталардағы орындалатын файлдардың негізінде, сіз бағдарламалар санатын құра аласыз және оны Бағдарламаны басқару құрамдасын конфигурациялау үшін пайдалана аласыз.

Таңдалған қалталардан орындалатын файлдарды қамтитын санатты құру үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

   Санаттар тізімі бар бет ашылады.

2. **Қосу** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

3. **Санатты жасау әдісін таңдау** қадамында санат атауын көрсетіп, **Белгілі бір қалтадағы орындалатын файлдарды қамтитын санат. Көрсетілген қалтаға көшірілген бағдарламалардың орындалатын файлдары автоматты түрде өңделеді және олардың метрикалық көрсеткіштері санатқа қосылады** параметрін таңдаңыз.

4. Орындалатын файлдары санатты құру үшін пайдаланылатын қалтаны көрсетіңіз.

5. Келесі параметрлерді конфигурациялаңыз:

   - **Санатқа динамикалық түрде қосылатын кітапханаларды (DLL) қосу**

     Бағдарламалар санатына динамикалық түрде қосылатын кітапханалар (DLL пішіміндегі файлдар) қосылады және Бағдарламаны басқару құрамдасы жүйеде іске қосылған осындай кітапханалардың әрекеттерін тіркейді. DLL пішіміндегі файлдарды санатқа қосу кезінде Kaspersky Security Center жұмысының өнімділігі төмендеуі мүмкін.

     Әдепкі бойынша, жалауша алынып тасталған.

   - **Санатқа скрипт туралы деректерді қосу**

     Бағдарлама санатына скрипт туралы деректер қосылады және скрипттер Веб-қауіптен қорғаныс құрамдасы тарапынан бұғатталмайды. Скрипт туралы деректерді санатқа қосу кезінде Kaspersky Security Center жұмысының өнімділігі төмендеуі мүмкін.

     Әдепкі бойынша, жалауша алынып тасталған.

   - **Хэш функциясын есептеу алгоритмі**: **Осы санаттағы файлдар үшін SHA256 мәнін есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан кейінгі нұсқаларында қолдау көрсетіледі) /Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)**

     Желіңіздегі құрылғыларға орнатылған қауіпсіздік бағдарламасы нұсқасына байланысты, санат файлдары үшін хеш функциясын Kaspersky Security Center бағдарламасы тарапынан есептеп шығару алгоритмін таңдау керек. Хэш функцияларымен есептелетін хэш мәндері туралы ақпарат басқару сервері дерекқорында сақталады.

SHA256 – алгоритмінде осалдық табылмаған криптографиялық хеш функциясы және ол қазіргі уақытта ең сенімді криптографиялық функция болып саналады. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы SHA256 хеш функциясын есептеп шығаруды қолдайды. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен нұсқалар үшін қолдау көрсетіледі.

Санат файлдары үшін Kaspersky Security Center бағдарламасы тарапынан хеш функциясын есептеп шығару нұсқаларының бірін таңдаңыз:

- Желіңізде орнатылған қауіпсіздік бағдарламаларының барлық даналары Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқасы болса, онда **SHA256** жалаушасын қойыңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан төмен бағдарлама нұсқалары үшін, орындалатын файлдың SHA256 өлшемшарты бойынша жасалған санатты қосу ұсынылмайды. Бұл қауіпсіздік бағдарламаның істен шығуына әкелуі мүмкін. Бұл жағдайда, санат файлдары үшін MD5 криптографиялық хеш функциясын қолдана аласыз.

- Сіздің желіңізде Kaspersky Endpoint Security 10 Service Pack 2 for Windows бағдарламасының ең ерте нұсқалары орнатылған болса, **MD5 хэші** тармағын таңдаңыз. Kaspersky Endpoint Security 10 Service Pack 2 for Windows және одан жоғары нұсқалары үшін орындалатын файлдың MD5 бақылау сомасының өлшемшарты бойынша жасалған санатты қосуға болмайды. Бұл жағдайда, санат файлдары үшін SHA256 криптографиялық хеш функциясын қолдана аласыз.

Желіңіздегі әртүрлі құрылғылар Kaspersky Endpoint Security 10 бағдарламасының ең ерте нұсқаларын да, ең кейінгі нұсқаларын да қолданса, онда **SHA256** жалаушасы мен **MD5 хэші** жалаушасын қойыңыз.

Әдепкі бойынша, **Санаттағы файлдар үшін SHA256 есептеп шығару (Kaspersky Endpoint Security 10 Service Pack 2 for Windows үшін қолдау көрсетіледі)** жалаушасы қойылған.

Әдепкі бойынша, **Осы санаттағы файлдар үшін MD5 есептеу (Kaspersky Endpoint Security 10 Service Pack 2 for Windows нұсқасынан бұрынғы нұсқалармен қолдау көрсетіледі)** алынып тасталған.

- **Қалтада өзгертулер бар-жоғын мәжбүрлеп сканерлеу**

  Егер бұл параметр қосулы болса, бағдарлама санаттарды толықтыру қалтасында өзгертулердің бар-жоғын мезгіл-мезгіл мәжбүрлеп тексереді. Тексерудің сағат түріндегі мерзімділігін жалаушаның жанындағы енгізу өрісінде көрсетуге болады. Әдепкі бойынша, мәжбүрлеп тексеру кезеңі 24 сағатқа тең келеді.

  Осы параметр өшірулі болса, қалтаны мәжбүрлеп тексеру орындалмайды. Сервер қалтадағы файлдарды өзгерту, қосу немесе жою кезінде оларға жүгінеді.

  Әдепкі бойынша, параметр өшірулі.

Шебердің жұмысы аяқталған кезде орындалатын файлдардың санаты жасалады. Ол санаттар тізімінде пайда болады. Бағдарламаны басқару құрамдасын конфигурациялау үшін санатты пайдалануға болады.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Бағдарлама санаттары тізімін қарап шығу

Сіз конфигурацияланған орындалатын файлдар санаттарының тізімін және әр санаттың параметрлерін көре аласыз.

Бағдарлама санаттары тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Операциялар → Үшінші тарап бағдарламалары → Бағдарлама санаттары** бөліміне өтіңіз.

Санаттар тізімі бар бет ашылады.

Бағдарлама санаты сипаттарын көру үшін,

санаттың атауын басыңыз.

Таңдалған санаттың сипаттар терезесі ашылады. Параметрлер бірнеше қойындыда топтастырылған.

Бағдарлама санатына оқиғамен байланысты орындалатын файлдарды қосу

Бағдарламаны басқару құрамдасы конфигурацияланғаннан кейін, Kaspersky Endpoint Security for Windows саясаттарында, оқиғалар тізімінде келесі оқиғалар көрсетілуі мүмкін:

- **Бағдарламаны іске қосуға тыйым салынған** (*Критикалық оқиға*). Егер сіз ережелерді қолдану үшін Бағдарламаны басқаруды конфигурациялаған болсаңыз, бұл оқиға көрсетіледі.
- **Бағдарламаны іске қосуға сынақ режиміне тыйым салынған** (*Ақпараттық* оқиға). Егер сіз сынақ режимінде ережелерді қолдану үшін Бағдарламаны басқаруды конфигурациялаған болсаңыз, бұл оқиға көрсетіледі.
- **Әкімшіге қолданбаның іске қосылуына тыйым салынғаны туралы хабар жіберу** (*Ескерту* оқиғасы). Егер сіз ережелерді қолдану үшін Бағдарламаны басқаруды конфигурациялаған болсаңыз, ал пайдаланушы іске қосу үшін бұғатталған бағдарламаға қатынасуды сұраса, бұл оқиға көрсетіледі.

Бағдарламаны басқару құрамдасына қатысты оқиғаларды көру үшін оқиғалар таңдауын жасау ұсынылады.

Бағдарламаны басқару оқиғаларына қатысты орындалатын файлдарды қолданыстағы бағдарламалар санатына немесе жаңа бағдарламалар санатына қосуға болады. Орындалатын файлдарды тек қолмен толтырылатын бағдарламалар санатына қосуға болады.

Бағдарламаны басқару құрамдасының оқиғаларымен байланысты орындалатын файлдарды бағдарламалар санатына қосу үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру → Оқиғаларды таңдау** бөліміне өтіңіз.

   Оқиғалар таңдауы тізімі көрсетіледі.

2. Бағдарламаны басқаруға қатысты оқиғаларды көру үшін оқиғалар таңдауын таңдап, сол оқиғалар таңдауын құруды іске қосыңыз.

   Бағдарламаны басқарумен байланысты оқиғалар таңдауын жасамаған болсаңыз, **Соңғы оқиғалар** сияқты алдын ала анықталған таңдауды таңдап, іске қосуға болады.

   Оқиғалар тізімі көрсетіледі.

3. Бағдарламалар санатына қосқыңыз келетін орындалатын файлдары бар оқиғаларды таңдап, **Санатқа тағайындау** түймесін басыңыз.

   Жаңа санат шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.

4. Шебер бетінде қажетті параметрлерді көрсетіңіз:

   - **Оқиғаға қатысты орындалатын файл бойынша әрекет** бөлімінде келесі опциялардың бірін таңдаңыз:

     - **Жаңа бағдарлама санатына қосу**

       Оқиғалармен байланысты орындалатын файлдар негізінде бағдарламалар санатын жасағыңыз келсе, осы параметрді таңдаңыз.

       Әдепкі бойынша, осы нұсқа таңдалған.

       Егер сіз осы параметрді таңдасаңыз, жаңа санаттың атын көрсетіңіз.

     - **Қолданыстағы бағдарлама санатына қосу**

       Бар бағдарламалар санатына оқиғаға қатысты орындалатын файлдарды қосқыңыз келсе, осы параметрді таңдаңыз.

       Әдепкі бойынша нұсқа таңдалмаған.

       Егер сіз осы параметрді таңдаған болсаңыз, орындалатын файлдарды қосқыңыз келетін қолмен толықтырылатын бағдарламалар санатын таңдаңыз.

   - **Ереже түрі** бөлімінде келесі нұсқалардың бірін таңдаңыз:

     - **Қамтылатындарға қосу ережелері**

     - **Шығарылатындарға қосу ережелері**

   - **Шарт ретінде пайдаланылатын параметр** бөлімінде келесі опциялардың бірін таңдаңыз:

     - **Сертификат мәліметтері (немесе сертификаты жоқ файлдар үшін SHA256 хэштері)**

       Файлдарға сертификат арқылы қол қоюға болады. Бұл арада, бір сертификатпен бірнеше файлға қол қоюға болады. Мысалы, бір бағдарламаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі бағдарламаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа бағдарламаның бірнеше нұсқасы немесе бір өндірушінің бірнеше бағдарламасы кіруі мүмкін.

       Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

       Санат ережелеріне орындалатын файл сертификатының деректерін немесе сертификаты жоқ файлдар үшін SHA256 хэш функциясын қосу қажет болса, осы нұсқаны таңдаңыз.

       Әдепкі бойынша, осы нұсқа таңдалған.

     - **Сертификат мәліметтері (сертификаты жоқ файлдар өткізіп жіберіледі)**

       Файлдарға сертификат арқылы қол қоюға болады. Бұл арада, бір сертификатпен бірнеше файлға қол қоюға болады. Мысалы, бір бағдарламаның әртүрлі нұсқаларына бір сертификатпен қол қоюға болады немесе бір өндірушінің бірнеше түрлі бағдарламаларына бір сертификатпен қол қоюға болады. Сертификатты таңдаған кезде санатқа бағдарламаның бірнеше нұсқасы немесе бір өндірушінің бірнеше бағдарламасы кіруі мүмкін.

       Санат ережелеріне орындалатын файл сертификатының деректерін қосу қажет болса, осы нұсқаны таңдаңыз. Орындалатын файлдың сертификаты болмаса, ондай файлды өткізіп жіберуге болады. Ол туралы ақпарат санатқа қосылмайды.

- **Тек SHA256 (хэші жоқ файлдар өткізіп жіберіледі)**

  Әрбір файлдың өзіндік бірегей SHA256 хэш функциясы бар. SHA256 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

  Санат ережелеріне тек орындалатын файлдың SHA256 хеш функциясының деректерін ғана қосу керек болса, осы нұсқаны таңдаңыз.

- **Тек MD5 (үзілген режим, тек Kaspersky Endpoint Security 10 Service Pack 1 нұсқасы үшін)**

  Әрбір файлдың өзіндік бірегей MD5 хэш функциясы бар. MD5 хэш функциясын таңдағанда, санатқа бағдарламаның белгіленген нұсқасы сияқты бір ғана тиісті файл кіреді.

  Санат ережелеріне тек орындалатын файлдың MD5 хеш функциясының деректерін ғана қосу керек болса, осы нұсқаны таңдаңыз. MD5 хеш функциясын есептеп шығаруға Kaspersky Endpoint Security 10 Service Pack 1 for Windows және одан да төмен нұсқалар үшін қолдау көрсетіледі.

5. **OK** түймесін басыңыз.

Шебердің жұмысы аяқталғаннан кейін, Бағдарламаны басқару оқиғаларымен байланысты орындалатын файлдар қолданыстағы бағдарламалар санатына немесе жаңа бағдарламалар санатына қосылады. Сіз өзгерткен немесе жасаған бағдарламалар санатының параметрлерін көре аласыз.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаларды басқару конфигурациялау

Бағдарламаны басқаруға арналған санаттарды жасағаннан кейін, оларды Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаны басқаруды конфигурациялау үшін пайдалануға болады.

Kaspersky Endpoint Security for Windows саясатындағы Бағдарламаны басқару құрамдасын конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

   Саясаттар тізімі бар бет көрсетіледі.

2. **Kaspersky Endpoint Security for Windows** саясатын басыңыз.

   Саясат сипаттары терезесі ашылады.

3. **Бағдарлама параметрлері** → **Қауіпсіздікті бақылау** → **Бағдарламаны басқару** бөліміне өтіңіз.

   Қолданбаның басқару параметрлері бар **Қолданбаны басқару** терезесі көрсетіледі.

4. **Бағдарламаны басқару** параметрі әдепкі бойынша қосулы. **Бағдарламаны басқару Өшірулі** қосқышы белсенді емес күйге ауыстырылғанына көз жеткізіңіз.

5. **Бағдарламаны басқару параметрлері** блогында Бағдарламаны басқару ережелерін қолдана отырып жұмыс режимін қосыңыз және Kaspersky Endpoint Security for Windows бағдарламасына бағдарламаларын іске қосуды бұғаттауға мүмкіндік беріңіз.

   Қолданбаның басқару ережелерін сынап көргіңіз келсе, **Қолданбаның басқару параметрлері** бөлімінде сынақ режимін қосыңыз. Сынақ режимінде Kaspersky Endpoint Security for Windows бағдарламасы қолданбалардың іске қосылуын бұғаттамайды, бірақ есепке іске қосылған ережелер туралы ақпаратты жазып алады. Осы ақпаратты қарау үшін **Есепті қарап шығу** сілтемесінен өтіңіз.

6. Пайдаланушылар бағдарламаларды іске қосқан кезде Kaspersky Endpoint Security for Windows бағдарламасы DLL модульдерін жүктеуді бақылағанын қаласаңыз, **DLL модульдерін жүктеуді басқару** параметрін қосыңыз.

   Модуль туралы ақпарат және модульді жүктеген бағдарлама есепте сақталады.

   Kaspersky Endpoint Security for Windows бағдарламасы тек **DLL модульдерін жүктеуді басқару** параметрі қосулы болғаннан кейін жүктелген DLL модульдер мен драйверлерді бақылайды. Kaspersky Endpoint Security for Windows барлық DLL модулі мен драйверін, соның ішінде Kaspersky Endpoint Security for Windows іске қосылғанға дейін жүктелгендерді басқарғанын қаласаңыз, **DLL модульдерін жүктеуді басқару** опциясын таңдағаннан кейін құрылғыны қайта іске қосыңыз.

7. (Қажет болса.) **Хабар үлгілері** блогында, бағдарлама іске қосу үшін бұғатталған кезде көрсетілетін хабар үлгісін және сізге жіберілетін электрондық пошта хабары үлгісін өзгертіңіз.

8. **Бағдарламаны басқару режимі** параметрлер блогында **Тыйым салу тізімі** немесе **Рұқсат ету тізімі** режимін таңдаңыз.

   Әдепкі бойынша **Тыйым салу тізімі** режимі таңдалған.

9. **Ереже тізімдері параметрлері** сілтемесінен өтіңіз.

   Бағдарлама санаттарын қосуға болатын **Тыйым салу және рұқсат ету тізімдері** терезесі ашылады. Әдепкі бойынша, **Тыйым салу тізімі** режимі таңдалған болса, **Тыйым салу тізімі** қойындысы немесе **Рұқсат ету тізімі** режимі таңдалған болса, **Рұқсат ету тізімі** режимі көрсетіледі.

10. **Тыйым салу және рұқсат ету тізімдері** терезесінде **Қосу** түймесін басыңыз.

    Бағдарламаны басқару ережесі терезесі ашылады.

11. **Өтініш, санатты таңдаңыз** сілтемесінен өтіңіз.

    Бағдарлама санаттары терезесі ашылады.

12. Бұрын жасаған бағдарламалар санатын (немесе санаттарын) қосыңыз.

    Өзгерту түймесін басу арқылы санат параметрлерін өзгертуге болады.

    Қосу түймесін басу арқылы санат жасауға болады.

    Жою түймесін басу арқылы санатты жоюға болады.

13. Бағдарлама санаттарының тізімін жасау аяқталғаннан кейін **OK** түймесін басыңыз.

    Бағдарлама санаты терезесі жабылады.

14. **Бағдарламаны басқару** ережесі терезесінде, **Субъектілер және олардың құқықтары** бөлімінде Бағдарламаны басқару ережелерін қолдану үшін пайдаланушылар мен пайдаланушылар топтарының тізімін жасаңыз.

15. Параметрлерді сақтау және **Бағдарламаны басқару ережесі** терезесін жабу үшін **OK** түймесін басыңыз.

16. Параметрлерді сақтау және **Тыйым салу және рұқсат ету тізімдері** терезесін жабу үшін **OK** түймесін басыңыз.

17. Параметрлерді сақтау және **Бағдарламаны басқару** ережесі терезесін жабу үшін **OK** түймесін басыңыз.

18. Kaspersky Endpoint Security for Windows саясаты параметрлері терезесін жабыңыз.

    Бағдарламаны басқару құрамдасы конфигурацияланған. Саясатты клиент құрылғыларына таратқаннан кейін, орындалатын файлдардың іске қосылуы бақыланады.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Клиент құрылғыларында орнатылған бағдарламалар тізімін алу және қарау

Kaspersky Security Center бағдарламасы, Linux және Windows операциялық жүйесінің басқаруымен жұмыс істейтін басқарылатын клиент құрылғыларында орнатылған бағдарламалық жасақтаманы түгендейді.

Желілік агент құрылғыда орнатылған бағдарламалар тізімін құрастырып, тізімді Басқару серверіне жібереді. Желілік агентке бағдарламалар тізімін жаңарту үшін шамамен 10-15 минут кетеді.

Windows операциялық жүйесі бар клиент құрылғылары үшін Желілік агент орнатылған бағдарламалар туралы ақпараттың көп бөлігін Windows тізімдемесінен алады. Linux операциялық жүйесі бар клиент құрылғылары үшін орнатылған бағдарламалар туралы ақпаратты Желілік агент пакет диспетчерлерінен алады.

> **Бағдарламалар тізімдемесі** бөлімдегі бағдарлама Linux операциялық жүйесі бар құрылғыда табылса, бағдарлама сипаттарында онымен байланысты орындалатын файлдар туралы ақпарат жоқ.

Басқарылатын құрылғыларда орнатылған бағдарламалар тізімін көру үшін,

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.

   Бетте басқарылатын құрылғыларда орнатылған бағдарламалары бар кесте көрсетіледі. Осы бағдарламаның сипаттарын көру үшін бағдарламаны таңдаңыз, мысалы: өндірушінің аты, нұсқа нөмірі, орындалатын файлдар тізімі, бағдарлама орнатылған құрылғылар тізімі, қолжетімді бағдарламалық жасақтама жаңартуларының тізімі немесе анықталған бағдарламалық жасақтама осалдықтарының тізімі.

2. Орнатылған бағдарламалары бар кесте деректерін келесідей топтастыруға және сүзуге болады:

   - Кестенің жоғарғы оң жақ бұрышындағы ( ) параметрлері белгішесін нұқыңыз.

     Ашылған **Бағандар параметрлері** мәзірінен кестеде көрсетілетін бағандарды таңдаңыз. Бағдарлама орнатылған клиент құрылғыларының операциялық жүйесінің түрін көру үшін **Операциялық жүйенің түрі** бағанын таңдаңыз.

- Кестенің жоғарғы оң жақ бұрышындағы ( ) сүзу белгішесін нұқыңыз, ашылған мәзірде сүзу критерийін көрсетіңіз және қолданыңыз.

  Орнатылған бағдарламалардың сүзілген кестесі көрсетіледі.

Таңдалған басқарылатын құрылғыда орнатылған бағдарламалар тізімін көру үшін,

Бағдарламаның негізгі терезесінде **Құрылғылар** → **Басқарылатын құрылғылар** → **<құрылғы атауы>** → **Кеңейтілген** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз. Бұл мәзірде бағдарламалар тізімін CSV немесе TXT пішіміндегі файлдарға экспорттауға болады.

Бағдарламаларды бақылау туралы толық ақпарат алу үшін анықтаманың келесі бөлімдерін қараңыз:

- Kaspersky Endpoint Security for Windows онлайн-анықтамасы
- Kaspersky Endpoint Security for Linux онлайн-анықтамасы
- Kaspersky Security for Virtualization Жеңіл агент
- Kaspersky Embedded Systems Security for Windows анықтамасы
- Kaspersky Embedded Systems Security for Linux анықтамасы

Kaspersky дерекқорынан үшінші тарап бағдарламасы үшін орнату пакетін жасау

Kaspersky Security Center Web Console сервері орнату пакеттері көмегімен үшінші тарап бағдарламаларын қашықтан орнатуды орындауға мүмкіндік береді. Осындай үшінші тарап бағдарламалары тиісті Kaspersky дерекқорына қосылған. Дерекқор, Жаңартуларды *Басқару серверінің қоймасына жүктеп алу* тапсырмасын бірінші рет іске қосу кезінде автоматты түрде жасалады.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетін жасау үшін:

1. Негізгі мәзірде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Орнату пакетін жасау шеберінің ашылған бетінде **Орнату пакетін жасау үшін Kaspersky дерекқорынан бағдарламаны таңдау** параметрін таңдап, **Келесі** түймесін басыңыз.
4. Ашылған бағдарламалар тізімінен тиісті бағдарламаны таңдап, **Келесі** түймесін басыңыз.
5. Ашылмалы тізімнен қажетті локализация тілін таңдап, **Келесі** түймесін басыңыз.

   Бұл қадам, бағдарлама бірнеше тілді ұсынса ғана көрсетіледі.

6. Сізге орнату үшін Лицензиялық келісімді қабылдау ұсынылатын болса, онда Лицензиялық келісімді оқып шығу үшін ашылған **Түпкі пайдаланушының лицензиялық келісімі** бетінде өндірушінің веб-сайтындағы сілтемеден өтіңіз, содан соң **Мен осы Түпкі пайдаланушының лицензиялық келісімінің ережелері мен шарттарын толық оқып шыққанымды, түсінгенімді және қабылдайтынымды растаймын** жалаушасын қойыңыз.

7. Ашылған **Жаңа орнату пакетінің атауы** бетінде, **Пакет атауы** өрісінде орнату пакетінің атауын көрсетіп, **Келесі** түймесін басыңыз.

Жасалған орнату пакеті Басқару серверіне жүктелгенше күтіңіз. Орнату пакетін жасау шебері сізге пакет жасау процесінің сәтті аяқталғанын білдіретін хабарды көрсеткеннен кейін, **Аяқтау** түймесін басыңыз.

Жасалған орнату пакеті орнату пакеттерінің тізімінде пайда болады. Сіз *Бағдарламаны қашықтан орнату* тапсырмасын жасау немесе қайта конфигурациялау кезінде осы пакетті таңдай аласыз.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлерін қарау және өзгерту

Егер сіз бұрын Kaspersky дерекқорында атап көрсетілген үшінші тарап бағдарламаларының қандай да бір орнату пакеттерін жасаған болсаңыз, онда сіз осы пакеттердің параметрлерін қарап, өзгерте аласыз.

Kaspersky дерекқорынан үшінші тарап бағдарламасының орнату пакетінің параметрлерін өзгерту жүйелік Осалдықтар мен патчтарды басқаруға арналған лицензия болған жағдайда ғана қолжетімді.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлерін қарау және өзгерту үшін:

1. Негізгі мәзірде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Орнату пакеттері** бөліміне өтіңіз.

2. Ашылған орнату пакеттері тізімінде тиісті пакеттің атын басыңыз.

3. Ашылған сипаттар бетінде қажет болса, параметрлерді өзгертіңіз.

4. **Сақтау** түймесін басыңыз.

Өзгерістер сақталды.

Kaspersky дерекқорынан үшінші тарап бағдарламасына арналған орнату пакетінің параметрлері

Үшінші тарап бағдарламасының орнату пакетінің параметрлері келесі қойындыларда топтастырылған:

Төменде берілген параметрлердің бір бөлігі ғана көрсетіледі. Осылайша **Сүзгі** түймесін басып, тізімнен тиісті бағаң атауларын таңдау арқылы қажетті бағандарды қоса аласыз.

- **Жалпы** қойыншасы:
  - Қолмен өзгертуге болатын орнату пакетінің атауын қамтитын енгізу өрісі.
  - **Бағдарлама**

    Орнату пакеті жасалған үшінші тарап бағдарламасының атауы.
  - **Нұсқа**

    Орнату пакеті жасалған үшінші тарап бағдарламасының нұсқа нөмірі.
  - **Өлшемі**

    Үшінші тарап бағдарламасына арналған орнату пакетінің өлшемі (килобайт түрінде).
  - **Жасалған күні**

    Үшінші тарап бағдарламасы үшін орнату пакетін жасау күні мен уақыты.
  - **Жолы**

    Үшінші тарап бағдарламасына арналған орнату пакеті орналасқан желілік қалтаға апаратын толық жол.
- **Орнату реті** қойыншасы:
  - **Қажетті жалпы жүйелік құрамдастарды орнату**

    Егер жалауша қойылса, жаңартуды орнатпас бұрын, бағдарлама автоматты түрде осы жаңартуды орнатуға қажетті барлық жалпыжүйелік құрамдастарды (алғышарттар) орнатады. Мысалы, мұндай алғышарттар операциялық жүйенің жаңартулары болуы мүмкін.

    Егер бұл параметр өшірулі болса, алғышарттарды қолмен орнату керек.

    Әдепкі бойынша, параметр өшірулі.
  - Жаңарту сипаттарын көрсететін және келесі бағандарды қамтитын кесте:
    - **Атауы**

      Жаңарту атауы.
    - **Сипаттама**

      Жаңарту сипаттамасы.

- **Көзі**

  Жаңарту көзі, яғни Microsoft немесе басқа үшінші тарап өндірушісі жаңартуды шығарды ма.

- **Түрі**

  Жаңарту түрі, яғни жаңарту драйверге немесе бағдарламаға арналған ба.

- **Санат**

  Microsoft жаңартулары үшін көрсетілетін Windows Server Жаңарту қызметтері (WSUS) санаттары (Критикалық жаңартулары, Анықтамалық жаңартулар, Драйверлер, Қосымша құрамдастардың пакеттері, Қауіпсіздік жаңартулары, Қызметтік пакеттер, Құралдар, Жинақтаушы жаңарту пакеттері, Жаңартулар немесе Алдыңғы нұсқалардың жаңартулары).

- **MSRC бойынша маңыздылық деңгейі**

  Microsoft Security Response Center (MSRC) анықтаған жаңартудың маңыздылық деңгейі.

- **Маңыздылық деңгейі**

  Kaspersky анықтаған жаңартудың маңыздылық деңгейі.

- **Патчтың маңыздылық деңгейі**

  Kaspersky бағдарламаларына арналған болса, патчтың маңыздылық деңгейі.

- **Мақала**

  Жаңарту сипаттамасы бар Білім базасындағы мақаланың идентификаторы.

- **Бюллетень**

  Жаңарту сипаттамасы бар қауіпсіздік бюллетені идентификаторы.

- **Орнатуға белгіленбеген (жаңа нұсқа)**

  Орнатуға белгіленбеген күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Орнатуға белгіленген**

  Орнатуға белгіленген күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Орнату**

  Орнатылуда күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Орнатылған**

  Орнатылған күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Сәтсіз аяқталды**

  Сәтсіз аяқталды күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Қайта іске қосу керек**

  Қайта іске қосу керек күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Тіркелген**

  Жаңарту тіркелген күн мен уақыт көрсетіледі.

- **Интерактивті түрде орнатылады**

  Жаңартуды орнату кезінде пайдаланушы тәжірибесі қажет пе екені көрсетіледі.

- **Қайтарып алынған**

  Жаңарту қайтарып алынғаны күн мен уақыт көрсетіледі.

- **Жаңартуды растау күйі**

  Жаңартуды орнатудың расталғаны/расталмағаны көрсетеді.

- **Тексеру**

  Жаңартудың ағымдағы шығарылымының нөмірі көрсетіледі.

- **Жаңарту идентификаторы**

  Жаңарту идентификаторы көрсетіледі.

- **Бағдарламаның нұсқасы**

  Бағдарлама жаңартылуы тиісті нұсқаның нөмірі көрсетіледі.

- **Ауыстырылып жатқан**

  Осы жаңартуды ауыстыра алатын басқа да жаңартулар көрсетіледі.

- **Ауыстыратын**

  Осы жаңартумен ауыстыруға болатын басқа да жаңартулар көрсетіледі.

- **Лицензиялық келісімнің шарттарын қабылдау керек**

  Лицензиялық келісімнің шарттарымен келісімді жаңарту керек пе екені көрсетіледі.

- **Сипаттамасының URL мекенжайы**

  Жаңарту өндірушісінің аты көрсетіледі.

- **Бағдарламалар тобы**

  Жаңарту қатысты болып табылатын бағдарламалар тобының аты көрсетіледі.

- **Бағдарлама**

  Жаңарту қатысты болып табылатын бағдарламаның аты көрсетіледі.

- **Локализация тілі**

  Жаңартудың локализация тілі көрсетіледі.

- **Орнатуға белгіленбеген (жаңа нұсқа)**

  Орнатуға белгіленбеген (жаңа нұсқа) күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Алғышарттарды орнатуды қажет етеді**

  Алғышарттарды орнатуды қажет етеді күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- **Жүктеп алу режимі**

  Жаңартуларды жүктеп алу режимі көрсетіледі.

- **Патч болып табылады**

  Жаңартудың патч болып табылады ма екені көрсетіледі.

- **Орнатылмаған**

  Орнатылмаған күйі жаңартылғаны/жаңартылмағаны көрсетіледі.

- Орнату кезінде пәрмен жолының параметрлері ретінде пайдаланылатын орнату пакетінің параметрлерін, олардың аттарын, сипаттамаларын және мәндерін көрсететін **Параметрлер** қойындысы. Егер пакетте мұндай параметрлер болмаса, тиісті хабар көрсетіледі. Осы параметрлердің мәндерін өзгертуге болады.

- Орнату пакетінің нұсқаларын көрсететін және келесі бағандарды қамтитын **Тексерістер журналы** қойындысы:

  - **Тексеру** – орнату пакетінің тексерісінің нөмірі.

  - **Уақыт** – орнату пакетінің параметрлерін өзгерту күні мен уақыты.

  - **Пайдаланушы** – орнату пакетінің параметрлерін өзгерткен пайдаланушының аты.

  - **Әрекет** – осы тексерісте орнату пакетімен орындалған әрекеттер.

  - **Сипаттама** – орнату пакеті параметрлерінің өзгерістерін тексеру сипаттамасы.

    Әдепкі бойынша, тексеру сипаттамасы толтырылмаған. Тексеру сипаттамасын қосу үшін қажетті тексеруді таңдап, **Сипаттаманы өңдеу** түймесін басыңыз. Ашылған терезеде тексеру сипаттамасы мәтінін енгізіңіз.

Бағдарлама тегтері

Kaspersky Security Center бағдарламасы бағдарламалар тізілімінен бағдарламаларға тегтерді тағайындауға мүмкіндік береді. Тег, бағдарламаларды топтастыру және іздеу үшін пайдалануға болатын бағдарлама белгісі болып саналады. Бағдарламаға тағайындалған тегті құрылғыларды таңдауға арналған шарттарда қолдануға болады.

Мысалы, [Шолғыштар] тегін жасап, оны Microsoft Internet Explorer, Google Chrome, Mozilla Firefox сияқты барлық шолғыштарға тағайындауға болады.

Бағдарлама тегтерін жасау

Бағдарлама тегін жасау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарлама тегтері** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Тег жасау терезесі көрсетіледі.
3. Тегті көрсетіңіз.
4. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

Жаңа жасалған тег бағдарлама тегтерінің тізімінде пайда болады.

Бағдарлама тегтерін өзгерту

Бағдарлама тегін қайта атау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарлама тегтері** бөліміне өтіңіз.
2. Атын өзгерткіңіз келетін тегтің жанындағы жалаушаны қойып, **Өңдеу** түймесін басыңыз.

   Тегтің сипаттары терезесі ашылады.
3. Тег атауын өзгертіңіз.
4. Өзгерістерін сақтау үшін **OK** түймесін басыңыз.

Жаңартылған тег бағдарлама тегтері тізімінде пайда болады.

Бағдарламаларға тегтер тағайындау

Бағдарламаға тегтер тағайындау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.
2. Тегтерді белгілеу қажет бағдарламаны таңдаңыз.
3. **Тегтер** қойыншасын таңдаңыз.

   Қойыншада Басқару серверінде бар барлық бағдарлама тегтері пайда болады. Таңдалған бағдарламаға тағайындалған тегтер **Тег белгіленді** бағанындағы жалаушалармен белгіленеді.

4. Тағайындау қажет тегтер үшін **Тег белгіленді** бағанындағы жалаушаларды қойыңыз.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Бағдарламаға тегтер белгіленді.

Бағдарламаларға тағайындалған тегтерді алып тастау

Бағдарламадан тегтерді алып тастау үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарламалар тізімдемесі** бөліміне өтіңіз.

2. Тегтерді алып тастау қажет бағдарламаны таңдаңыз.

3. **Тегтер** қойыншасын таңдаңыз.

   Қойыншада Басқару серверінде бар барлық бағдарлама тегтері пайда болады. Таңдалған бағдарламаға тағайындалған тегтер **Тег белгіленді** бағанындағы жалаушалармен белгіленеді.

4. Алып тастау қажет тегтер үшін **Тег белгіленді** бағанындағы жалаушаларды алып тастаңыз.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Тегтер бағдарламадан алынады.

Бағдарламалардан алынған тегтер жойылмайды. Қажет болса, оларды қолмен жоюға болады.

Бағдарлама тегтерін жою

Бағдарлама тегін жою үшін:

1. Бағдарламаның негізгі терезесінде **Операциялар** → **Үшінші тарап бағдарламалары** → **Бағдарлама тегтері** бөліміне өтіңіз.

2. Тізімнен жойғыңыз келетін бағдарлама тегтерін таңдаңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде **OK** түймесін басыңыз.

Таңдалған бағдарлама тегі жойылды. Жойылған тег, ол тағайындалған барлық бағдарламалардан автоматты түрде алынып тасталады.

Бақылау және есеп беру

Бұл бөлімде, Kaspersky Security Center бағдарламасында есептермен жұмыс істеу және мониторинг жүргізу функциялары сипатталған. Бұл функциялар желіңіздің инфрақұрылымы, қорғаныс күйі, сондай-ақ статистика туралы мәлімет алуға мүмкіндік береді.

Kaspersky Security Center бағдарламасын орналастыру немесе оның жұмыс істеуі барысында мониторинг функцияларын және есеп параметрлерін конфигурациялауға болады.

Сценарий: Бақылау және есеп беру

Бұл бөлімде Kaspersky Security Center бағдарламасында бақылау және есеп беру конфигурациясы сценарийі берілген.

Алдын ала талаптар

Kaspersky Security Center бағдарламасын ұйымның желісіне орналастырғаннан кейін, сіз Kaspersky Security Center көмегімен желінің қауіпсіздік күйін мониторингтеуге және есептерді қалыптастыруға кірісе аласыз.

Ұйымның желісіндегі бақылау және есептермен жұмыс келесі кезеңдерден тұрады:

1. **Құрылғылардың күйлерін ауыстыруды конфигурациялау**

   Нақты жағдайларға байланысты құрылғы күйлері параметрлерімен танысыңыз. Осы параметрлерді өзгерту арқылы, сіз *Критикалық* немесе *Ескерту* маңызды деңгейлері бар оқиғалар санын өзгерте аласыз. Құрылғының күйін ауыстырып қосуды конфигурациялау кезінде мынаны тексеріңіз:

   - жаңа параметрлер сіздің ұйымыңыздың ақпараттық қауіпсіздік саясатына қарама-қайшы келмейді;
   - сіз өз ұйымыңыздың желісіндегі маңызды қауіпсіздік оқиғаларына уақтылы жауап бере аласыз.

2. **Клиент құрылғыларындағы оқиғалар туралы хабарландыру параметрлерін конфигурациялау**

   Нұсқаулар:

   Клиент құрылғыларындағы оқиғалар туралы хабарландыруларды (электрондық пошта, SMS немесе орындалатын файлды іске қосу арқылы) конфигурациялау.

3. **Қауіпсіздік желіңіздің Вирустық шабуыл оқиғасына жауабын өзгерту**

   Басқару сервері сипаттарындағы шекті мәндерді өзгертуге болады. Белсендірілетін аса қатаң саясатты жасай аласыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасай аласыз.

4. **Критикалық және ескерту хабарландырулары үшін ұсынылатын әрекеттерді орындау**

   Нұсқаулар:

   Ұйымыңыздың желісі үшін ұсынылатын әрекеттерді орындаңыз.

5. **Ұйымыңыздың желі қауіпсіздігі күйін қарау**

Нұсқаулар:

- Қорғаныс күйі веб-виджетін қарау.
- Қорғаныс жағдайы туралы есеп есебін жасау және қарау.
- Қателер туралы есеп есебін жасау және қарау.

6. **Қорғалмаған клиент құрылғыларын табу**

   Нұсқаулар:

   - Жаңа құрылғылар веб-виджетін қарау.
   - Қорғанысты орналастыру туралы есеп есебін жасау және қарау.

7. **Клиент құрылғылары қорғанысын тексеру**

   Нұсқаулар:

   - Қорғаныс күйі және Қауіптер статистикасы санаттарынан есепті жасау және қарау.
   - Критикалық оқиғалар таңдауын іске қосу және қарау.

8. **Дерекқорға оқиғаларды жүктеуді бағалау және шектеу**

   Басқарылатын бағдарламалар жұмыс істеп тұрған кезде туындайтын оқиғалар туралы ақпарат клиент құрылғысынан беріледі және Басқару серверінің дерекқорында тіркеледі. Басқару серверіне түсетін жүктемені азайту үшін дерекқорда сақталуы мүмкін оқиғалардың ең көп санын бағалаңыз және шектеңіз.

   Нұсқаулар:

   - Дерекқорда орынды есептеу
   - Оқиғалардың ең көп санын шектеу

9. **Лицензия мәліметтерін қарау**

   Нұсқаулар:

   - Бақылау тақтасына Лицензиялық кілтті пайдалану веб-виджетін қосу және қарау
   - Лицензиялық кілттерді пайдалану туралы есеп есебін жасау және қарау

Нәтижелер

Сценарий аяқталғаннан кейін, сіз өз ұйымыңыздың желісін қорғау туралы хабардар боласыз және осылайша, одан әрі қорғау үшін әрекеттерді жоспарлай аласыз.

Бақылау түрлері және есеп беру туралы

Ұйым желісіндегі қауіпсіздік оқиғалары туралы ақпарат Басқару сервері дерекқорында сақталады. Kaspersky Security Center Web Console веб-консолі ұйымыңыздың желісінде бақылау және есеп берудің келесі түрлерін ұсынады:

- Бақылау тақтасы
- Есептер
- Оқиғалар таңдау
- Хабарландырулар

Бақылау тақтасы

Бақылау тақтасы ақпаратты графикалық түрде ұсыну арқылы ұйымның желісіндегі қауіпсіздік күйін бақылауға мүмкіндік береді.

Есептер

Есептер бұл ақпаратты файлға сақтау, электрондық пошта арқылы жіберу және басып шығару үшін ұйымыңыздың желісінің қауіпсіздігі туралы толық сандық ақпаратты алуға мүмкіндік береді.

Оқиғалар таңдау

Оқиғаларды таңдау, экранда Басқару серверінің дерекқорынан таңдалған аталған оқиғалар жиынтығын көруге арналған. Осы оқиға түрлері келесі санаттар бойынша топтастырылған:

- Маңыздылық деңгейі: **Критикалық оқиғалар**, **Функциялық ақаулар**, **Ескертулер** және **Ақпараттық оқиғалар**.
- Уақыт: **Соңғы оқиғалар**.
- Түрі: **Пайдаланушылардың сұраулары** және **Аудит оқиғалары**.

Kaspersky Security Center Web Console интерфейсінде конфигурациялауға қолжетімді параметрлер негізінде пайдаланушы тарапынан айқындалған оқиғалар таңдауын жасай аласыз және көре аласыз.

Хабарландырулар

Хабарландырулар оқиғалар туралы ескертуге және сіз сәйкес деп санайтын ұсынылған әрекеттерді орындау арқылы осы оқиғаларға жауап беру жылдамдығыңызды арттыруға көмектесу үшін жасалған.

Бақылау тақтасы және веб-виджеттер

Бұл бөлімде бақылау тақтасы және бақылау тақтасында көрсетілген веб-виджеттер туралы ақпарат бар. Бөлімде веб-виджеттерді басқару және веб-виджеттерді конфигурациялау бойынша нұсқаулар бар.

Бақылау тақтасын қолдану

Бақылау тақтасы ақпаратты графикалық түрде ұсыну арқылы ұйымның желісіндегі қауіпсіздік күйін бақылауға мүмкіндік береді.

Бақылау тақтасы Kaspersky Security Center Web Console бағдарламасында **Бақылау және есеп беру → Бақылау тақтасы** бөлімінде қолжетімді.

Бақылау тақтасында конфигурацияланатын веб-виджеттер бар. Сіз дөңгелек диаграммалар, кестелер, графиктер, гистограммалар және тізімдер түрінде ұсынылған көптеген веб-виджеттерді таңдай аласыз. Веб-виджеттерде көрсетілген ақпарат автоматты түрде жаңартылады, жаңарту кезеңі бір-екі минутты құрайды. Жаңартулар арасындағы уақыт аралығы веб-виджет түріне байланысты өзгереді. Веб-виджет деректерін кез келген уақытта мәзір арқылы қолмен жаңартуға болады.

Әдепкі бойынша, веб-виджеттер Басқару сервері дерекқорында сақталатын оқиғалар туралы ақпаратты қамтиды.

Әдепкі бойынша, Kaspersky Security Center Web Console бағдарламасы келесі санаттарға арналған веб-виджеттер жиынтығына ие:

- **Қорғаныс күйі**
- **Орналастыру**
- **Жаңарту**
- **Қауіптер статистикасы**
- **Басқа**

Кейбір веб-виджеттерде сілтемелі мәтін бар. Толық ақпаратты көру үшін мына сілтемеге өтіңіз.

Бақылау тақтасын конфигурациялау кезінде қажетті веб-виджеттерді қосуға, веб-виджеттерді жасыруға, сондай-ақ веб-виджеттердің сыртқы түрін немесе өлшемін өзгертуге, веб-виджеттерді жылжытуға және веб-виджеттердің параметрлерін өзгертуге болады.

Ақпараттық тақтаға веб-виджетті қосу

Веб-виджетті ақпараттық тақтаға қосу үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.
2. **Веб-виджетті қосу не қалпына келтіру** түймесін басыңыз.
3. Қолжетімді веб-виджеттер тізімінен ақпараттық тақтаға қосу қажет веб-виджетті таңдаңыз.

   Веб-виджеттер санаттар бойынша топтастырылған. Санатқа қандай веб-виджеттердің кіретінін көру үшін санаттың атауы жанындағы шеврон (>) белгішесін басыңыз.
4. **Қосу** түймесін басыңыз.

Таңдалған веб-виджеттер ақпараттық тақтаның соңына қосылады.

Қосылған веб-виджеттердің сыртқы түрі мен параметрлерін өзгертуге болады.

Веб-виджетті ақпараттық тақтадан жою

Веб-виджетті ақпараттық тақтадан жою үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.
2. Жою қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. **Веб-виджетті жасыру** таңдаңыз.
4. Пайда болған **Ескерту** терезеде **ОК** түймесін басыңыз.

Таңдалған веб-виджет ақпараттық тақтадан жойылады. Алдағыда, веб-виджетті ақпараттық тақтаға қайтадан қосуға болады.

Веб-виджетті ақпараттық тақтадан жылжыту

Веб-виджетті ақпараттық тақтадан жылжыту үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.
2. Жылжыту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. **Жылжыту** таңдаңыз.
4. Веб-виджетті жылжыту қажет орынды көрсетіңіз. Тек басқа веб-виджетті таңдауға болады.

Таңдалған веб-виджеттер орындарын ауыстырады.

Виджеттің өлшемін немесе сыртқы түрін өзгерту

Веб-виджеттердің сыртқы түрін өзгертуге болады: бағаналы немесе сызықтық диаграмманы таңдаңыз. Кейбір веб-виджеттер үшін өлшемін өзгертуге болады: шағын, орташа немесе ірі.

Веб-виджеттің сыртқы түрін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз.
2. Өзгерту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. Келесі әрекеттердің бірін орындаңыз:
   - Веб-виджет бағандық диаграмма ретінде көрсетілуі үшін **Сызба түрі: жолақтар** тармағын таңдаңыз.
   - Веб-виджет сызықтық диаграмма ретінде көрсетілуі үшін **Сызба түрі: Жолдар** тармағын таңдаңыз.
   - Веб-виджет алып жатқан аймақтың өлшемін ауыстыру үшін келесі мәндердің бірін таңдаңыз:
     - **Ықшам**
     - **Ықшам (тек жолақ)**
     - **Орташа (сақиналы сызба)**
     - **Орташа (гистограмма)**
     - **Максимум**

Таңдалған веб-виджеттің сыртқы түрі өзгертіледі.

Веб-виджет параметрлерін өзгерту

Веб-виджет параметрлерін өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз.
2. Өзгерту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. **Параметрлерді көрсету** таңдаңыз.
4. Ашылған веб-виджет параметрлері терезесінде веб-виджеттің қажетті параметрлерін өзгертіңіз.
5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Таңдалған веб-виджеттің параметрлері өзгертіледі.

Параметрлер жиынтығы нақты веб-виджетке байланысты. Төменде кейбір жалпы параметрлер берілген:

- **Веб-виджет ауқымы** – веб-виджет ақпаратты көрсететін нысандар жиынтығы; мысалы, басқару тобы немесе құрылғылар таңдауы.
- **Тапсырманы таңдау** – веб-виджет ақпаратты көрсететін тапсырма.
- **Уақыт аралығы** – веб-виджетте ақпарат көрсетілетін кезең; мысалы, белгіленген күннен бастап қазіргі уақытқа дейін немесе көрсетілген күндер саны ішінде қазіргі уақытқа дейін белгіленген екі күн арасында.
- **Осы кезде Критикалыққа орнату** және **Осы кезде Ескертуге орнату** – күй графигінде түстер тағайындалатын ережелер.

Веб-виджет параметрлерін өзгерткеннен кейін веб-виджет деректерін қолмен жаңартуға болады.

Веб-виджет деректерін жаңарту үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру → Бақылау тақтасы** бөліміне өтіңіз.
2. Жылжыту қажет веб-виджеттің жанындағы параметрлер (⚙) белгішесін басыңыз.
3. **Жаңарту** түймесін басыңыз.

Веб-виджет деректері жаңартылды.

Тек бақылау тақтасын қарау режимі туралы

Желіні басқармайтын, бірақ Kaspersky Security Center-де желі қорғанысы статистикасын көргісі келетін қызметкерлер үшін Тек бақылау тақтасын қарау режимін конфигурациялауға болады (мысалы, бұл топ-менеджер болуы мүмкін). Пайдаланушыда осы режим қосулы болғанда, пайдаланушыда алдын ала анықталған веб-виджеттер жиынтығы бар бақылау тақтасы ғана көрсетіледі. Осылайша, пайдаланушы веб-виджеттерде көрсетілген статистиканы, мысалы, барлық басқарылатын құрылғылардың қорғаныс күйін, жақында табылған қауіптер санын немесе желідегі ең көп таралған қауіптер тізімін көре алады.

Пайдаланушы Тек бақылау тақтасын қарау режимінде жұмыс істеген кезде келесі шектеулер қолданылады:

- Бас мәзір көрсетілмейді, сондықтан пайдаланушы желіні қорғау параметрлерін өзгерте алмайды.
- Пайдаланушы веб-виджеттермен байланысты әрекеттерді орындай алмайды, мысалы, оларды қоса немесе жасыра алмайды. Сондықтан, пайдаланушыға қажет барлық веб-виджеттерді бақылау тақтасына орналастырып, оларды конфигурациялау керек, мысалы, нысандарды санау ережесін белгілеу немесе кезеңді көрсету қажет.

Сіз "Тек бақылау тақтасы" режимін өзіңізге тағайындай алмайсыз. Егер осы режимде жұмыс істегіңіз келсе, жүйе әкімшісіне, провайдерге (MSP) немесе **Жалпы функциялар: Пайдаланушы құқықтары** функционалдық аймағында **Нысан ACL параметрлерін өзгерту** құқықтары бар пайдаланушыға жүгініңіз.

Тек бақылау тақтасын қарау режимін конфигурациялау

Тек бақылау тақтасын қарау режимін конфигурациялауды бастау алдында, келесі алдын ала талаптардың орындалғанына көз жеткізіңіз:

- Сізде **Жалпы функциялар: Пайдаланушы құқықтары** функционалды аймағында **Modify object ACLs** құқығы бар. Егер сізде бұл құқық болмаса, режимді конфигурациялау үшін қойынша болмайды.
- **Жалпы функционал: Базалық функционал** аймағындағы **Оқу** құқығы бар пайдаланушы.

> Егер сіздің желіңізде Басқару серверлері иерархиясы құрылған болса, Тек бақылау тақтасын қарау режимін конфигурациялау үшін **Пайдаланушылар** в разделе **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөлімінде пайдаланушы есептік жазбасы қолжетімді Серверге өтіңіз. Бұл басты Сервер немесе физикалық қосалқы Сервер болуы мүмкін. Виртуалды Басқару серверінде "Тек бақылау тақтасы" режимін конфигурациялау мүмкін емес.

"Тек бақылау тақтасы" режимін конфигурациялау үшін:

1. Қолданбаның негізгі терезесінде **Пайдаланушылар және рөлдер** → **Пайдаланушылар және топтар** бөліміне өтіп, **Пайдаланушылар** қойындысын таңдаңыз.
2. Веб-виджеттері бар құралдар тақтасын конфигурациялағыңыз келетін пайдаланушы есептік жазбасының атын басыңыз.
3. Есептік жазба сипаттары терезесі ашылғанда **Бақылау тақтасы** қойыншасын таңдаңыз.

   Ашылған қойыншада пайдаланушыға да арналған бақылау тақтасын көрсетіледі.
4. **"Тек бақылау тақтасы" режимін көрсету** параметрі қосулы болса, оны қосқыш арқылы өшіріңіз.

   Бұл параметр қосылған кезде де бақылау тақтасын өзгерту мүмкін емес. Параметрді өшіргеннен кейін веб-виджеттерді басқаруға болады.
5. Бақылау тақтасының сыртқы түрін конфигурациялаңыз. **Бақылау тақтасы** қойыншасында дайындалған веб-виджеттер жиынтығы, конфигурацияланатын есептік жазбасы бар пайдаланушы үшін қолжетімді. Мұндай есептік жазбасы бар пайдаланушы веб-виджеттердің параметрлерін немесе өлшемін өзгерте алмайды, бақылау тақтасына веб-виджеттерді қоса алмайды немесе одан жоя алмайды. Сондықтан, оларды желіні қорғау статистикасын көре алатындай етіп пайдаланушыға бейімдеп конфигурациялаңыз. Осы мақсатта, **Бақылау тақтасы** қойыншасында **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміндегідей әрекеттерді орындауға болады:
   - Бақылау тақтасына веб-виджеттерді қосу.
   - Пайдаланушыға қажет емес веб-виджеттерді жасыру.
   - Белгіленген тәртіпте веб-виджеттерді жылжыту.
   - Веб-виджеттердің өлшемін немесе сыртқы түрін өзгерту.
   - Веб-виджет параметрлерін өзгерту.
6. **"Тек бақылау тақтасы" режимін көрсету** параметрін қосу үшін қосқышты ауыстырып қосыңыз.

Осыдан кейін, пайдаланушыға тек бақылау тақтасы қолжетімді болады. Пайдаланушы статистиканы көре алады, бірақ желіні қорғау параметрлерін және бақылау тақтасының сыртқы түрін өзгерте алмайды. Пайдаланушы үшін бірдей бақылау тақтасы көрсетілгендіктен, сіз бақылау тақтасын да өзгерте алмайсыз.

Бұл параметрді өшірулі күйде қалдырсаңыз, пайдаланушыда бас мәзір көрсетіледі, сондықтан ол Kaspersky Security Center бағдарламасында әртүрлі әрекеттерді орындай алады, соның ішінде қауіпсіздік параметрлері мен веб-виджеттерді өзгерте алады.

7. Тек бақылау тақтасын қарау режимін конфигурациялауды аяқтағаннан кейін **Сақтау** түймесін басыңыз. Осыдан кейін ғана дайындалған бақылау тақтасы пайдаланушыда көрсетіледі.

8. Егер пайдаланушы қолдау көрсетілетін Kaspersky бағдарламаларының статистикасын көргісі келсе және оған қатынасу құқығы қажет болса, сол пайдаланушыға құқықтарды конфигурациялаңыз. Осыдан кейін, Kaspersky бағдарламаларының деректері пайдаланушыда осы бағдарламалардың веб-виджеттерінде көрсетіледі.

Енді пайдаланушы Kaspersky Security Center бағдарламасына конфигурацияланатын есептік жазбамен кіре алады және Тек бақылау тақтасын қарау режимінде желіні қорғау статистикасын көре алады.

Басқару және қорғау есептері

Бұл бөлімде есептерді пайдалану, пайдаланушы есептерінің үлгілерін басқару, есептерді жасау үшін үлгілерді пайдалану және есептерді жеткізу тапсырмаларын жасау тәсілі сипатталған.

Есептерді қолдану

Есептер бұл ақпаратты файлға сақтау, электрондық пошта арқылы жіберу және басып шығару үшін ұйымыңыздың желісінің қауіпсіздігі туралы толық сандық ақпаратты алуға мүмкіндік береді.

Есептер Kaspersky Security Center Web Console бағдарламасында **Бақылау және есеп беру** → **Есептер** бөлімінде қолжетімді.

Әдепкі бойынша, есептер соңғы 30 күндегі ақпаратты қамтиды.

Әдепкі бойынша, Kaspersky Security Center бағдарламасы келесі санаттарға арналған есептер жиынтығына ие:

- **Қорғаныс күйі**
- **Орналастыру**
- **Жаңарту**
- **Қауіптер статистикасы**
- **Басқа**

Сіз пайдаланушылық есеп үлгілерін жасай аласыз, есеп үлгілерін өңдеп, жоя аласыз.

Есептерді қолданыстағы үлгілер негізінде жасай аласыз, есептерді файлға экспорттай аласыз және есептерді жеткізу тапсырмаларын жасай аласыз.

Есеп үлгісін жасау

Есеп үлгісін жасау үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Нәтижесінде, есеп үлгісін жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
3. Есептің атауын енгізіп, есеп түрін таңдаңыз.
4. Шебердің **Әрекет ету ауқымы** қадамында, осы үлгі негізінде жасалған есептерде көрсетілетін деректері бар клиент құрылғылары жиынтығын таңдаңыз (басқару топтары, құрылғылар таңдауы немесе барлық желілік құрылғылар).
5. Шебердің **Хабарлау мерзімі** бетінде есеп жасалатын кезеңді көрсетіңіз. Қолжетімді мәндері:

   - екі көрсетілген күн арасында;
   - көрсетілген күннен есеп жасалған күнге дейін;
   - есеп жасалған күннен бастап, минус көрсетілген күндер саны, есеп жасалған күнге дейін.

   Кейбір есептерде бұл бет көрсетілмеуі мүмкін.
6. Шебердің жұмысын аяқтау үшін **OK** түймесін басыңыз.
7. Келесі әрекеттердің бірін орындаңыз:

   - Жаңа есеп үлгісін сақтау және оның негізінде есеп жасауды бастау үшін **Сақтау және іске қосу** түймесін басыңыз.

     Есеп үлгісі сақталады. Есеп құрастырылады.
   - Жаңа есеп үлгісін сақтау үшін **Сақтау** түймесін басыңыз.

     Есеп үлгісі сақталады.

Жасалған үлгіні есептерді қалыптастыру және қарау үшін пайдалануға болады.

Есеп үлгісінің сипаттарын қарау және өзгерту

Есеп үлгісінің негізгі сипаттарын, мысалы, есеп үлгісінің атауын немесе есепте көрсетілетін өрістерді қарауға және өзгертуге болады.

Есеп үлгісінің сипаттарын қарау және өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.
2. Сипаттарын көргіңіз және өзгерткіңіз келетін есеп үлгісіне қарама-қарсы жалауша қойыңыз.

   Балама ретінде, алдымен есепті құрастырып, кейін **Өңдеу** түймесін басуға болады.

3. **Есеп үлгісінің сипаттарын ашу** түймесін басыңыз.

   Жалпы қойыншасында **<есеп атауы> есебін өзгерту** терезесі ашылады.

4. Есеп үлгісі сипаттарын өзгертіңіз:

   - **Жалпы** қойыншасы:

     - Есеп үлгісінің атауы

     - **Көрсетілетін жазбалардың ең көп саны**

       Егер бұл параметр қосылса, есептің егжей-тегжейлі деректері бар кестеде көрсетілетін жазбалар саны көрсетілген мәннен аспайды.

       Есеп жазбалары алдымен есеп үлгісі сипаттарының **Өрістер** → **Мәліметтер өрістері** бөлімінде көрсетілген ережелерге сай сұрыпталады, содан соң қорытқы жазбалардың бірінші бөлігі ғана сақталады. Есептің егжей-тегжейлі деректері бар кесте тақырыбында, көрсетілетін жазбалар саны және есеп үлгісінің басқа параметрлеріне сәйкес келетін жазбалардың жалпы саны көрсетілген.

       Егер бұл параметр өшірулі болса, есептің егжей-тегжейлі деректері бар кестеде барлық жазбалар көрсетіледі. Бұл параметрді өшіру ұсынылмайды. Көрсетілетін есеп жазбаларының санын шектеу дерекқорды басқару жүйесіне түсетін жүктемені және есепті қалыптастыру мен экспорттауға кететін уақытты азайтады. Кейбір есептерде тым көп жазбалар бар. Мұндай жағдайларда барлық жазбаларды қарау және талдау тым көп еңбекті қажет етуі мүмкін. Сондай-ақ мұндай есепті жасау кезінде құрылғыңыздың жады таусылуы мүмкін, демек есепті көре алмайсыз.

       Әдепкі бойынша, параметр қосулы. Әдепкі бойынша, 1000 мәні көрсетілген.

     - **Топ**

       Есеп жасалатын клиент құрылғылары жиынтығын өзгерту үшін **Параметрлер** түймесін басыңыз. Есептердің кейбір түрлері үшін түйме қолжетімді болмауы мүмкін. Нақты деректер есеп үлгісін жасау кезінде көрсетілген параметрлер мәндеріне байланысты.

     - **Уақыт аралығы**

       Есеп жасалатын кезеңді өзгерту үшін **Параметрлер** түймесін басыңыз. Есептердің кейбір түрлері үшін түйме қолжетімді болмауы мүмкін. Қолжетімді мәндері:

       - екі көрсетілген күн арасында;
       - көрсетілген күннен есеп жасалған күнге дейін;
       - есеп жасалған күннен бастап, минус көрсетілген күндер саны, есеп жасалған күнге дейін.

     - **Қосалқы және виртуалды Басқару серверлерінен алынған деректерді қамту**

       Бұл параметр өшірулі болса, есеп есеп үлгісі жасалған Басқару серверіне бағынатын қосалқы және виртуалды Басқару серверлерінен алынған ақпаратты қамтиды.

       Тек ағымдағы Басқару серверінің деректерін ғана қарағыңыз келсе, осы параметрді өшіріңіз.

       Әдепкі бойынша, параметр қосулы.

     - **Кірістіру деңгейіне дейін**

       Есепте, ағымдағы Басқару серверінің астында, көрсетілген мәннен төмен немесе оған тең тіркеме деңгейінде орналасқан қосалқы және виртуалды Басқару серверлерінің деректері бар.

       Әдепкі бойынша, 1 мәні көрсетілген. Егер сіз есепте ағаштың ең төменгі деңгейінде орналасқан қосалқы Басқару серверлері туралы ақпаратты көргіңіз келсе, бұл мәнді өзгерте аласыз.

- **Деректерді күту уақыт аралығы (мин)**

  Есеп үлгісі жасалған Басқару сервері есепті жасау үшін көрсетілген уақыт ішінде қосалқы Басқару серверлерінен деректерді күтеді. Егер деректер көрсетілген уақыт аралығында қосалқы Басқару серверінен алынбаса, есеп кез келген жағдайда іске қосылады. Есепте нақты деректердің орнына кэштен алынған деректер (егер **Қосалқы Басқару серверлерінен алынған деректерді кэштеу** параметрі қосулы болса) не болмаса **N/A** (қолжетімді емес) көрсетіледі.

  Әдепкі бойынша күту уақыты – 5 минут.

- **Қосалқы Басқару серверлерінен алынған деректерді кэштеу**

  Қосалқы Басқару серверлері деректерді үнемі есеп үлгісі жасалған негізгі Басқару серверіне жібереді. Берілген деректер кэште сақталады.

  Басқару сервері есепті құру кезінде қосалқы Басқару серверінің деректерін ала алмаса, есеп кэштегі деректерді көрсетеді. Бұл жағдайда, деректер кэшке жіберілген күн көрсетіледі.

  Бұл параметрді қосу арқасында өзекті деректерді алу мүмкін болмаса да, қосалқы Басқару серверлерінен алынған ақпаратты көруге мүмкіндік беріледі. Алайда, көрсетілетін деректер ескірген болуы мүмкін.

  Әдепкі бойынша, параметр өшірулі.

- **Кэшті жаңарту жиілігі (сағ)**

  Қосалқы Басқару серверлері деректерді үнемі есеп үлгісі жасалған негізгі Басқару серверіне жібереді. Сіз осы кезеңді сағат түрінде көрсете аласыз. Егер 0 мәні белгіленсе, деректер тек есеп шығару кезінде беріледі.

  Әдепкі бойынша, 0 мәні көрсетілген.

- **Қосалқы Басқару серверлерінен толық ақпаратты жіберу**

  Жасалған есепте егжей-тегжейлі деректер кестесі есеп үлгісі жасалған негізгі Басқару серверінің қосалқы Басқару серверлерінен алынған ақпаратты қамтиды.

  Егер бұл параметр қосылса, онда есепті құру баяулайды және Басқару серверлері арасындағы трафик артады. Дегенмен, сіз барлық деректерді бір есепте көре аласыз.

  Бұл параметрді қоспау үшін сіз ақаулы қосалқы Басқару серверін табу үшін есеп деректерін талдай аласыз, содан кейін бірдей есепті тек сол ақаулы Басқару сервері үшін жасай аласыз.

  Әдепкі бойынша, параметр өшірулі.

- **Өрістер** қойынша

  Есепте көрсетілетін өрістерді таңдап, осы өрістердің ретін өзгерту үшін **Жоғары жылжыту** және **Төменге жылжыту** түймелерін пайдаланыңыз. **Қосу** және **Өңдеу** түймелерінің көмегімен есептегі ақпарат таңдалған өрістер бойынша сүзгіленетінін немесе сұрыпталатынын көрсетіңіз.

  Сондай-ақ, **Мәліметтер өрісінің сүзгілері** бөлімінде, кеңейтілген сүзгілеу пішімін қолдана бастау үшін **Түрлендіру сүзгілері** түймесін баса аласыз. Бұл пішім логикалық НЕМЕСЕ көмегімен әртүрлі өрістерде көрсетілген сүзгілеу шарттарын біріктіруге мүмкіндік береді. **Түрлендіру сүзгілері** түймесін басқаннан кейін, оң жақта тақта ашылады. Лицензияны қайтарып алуды растайтын **Түрлендіру сүзгілері** түймесін басыңыз. Енді сіз логикалық НЕМЕСЕ көмегімен қолданылатын **Мәліметтер өрістері** бөлімінен шарттары бар түрлендірілген сүзгіні анықтай аласыз.

  Есепті күрделі сүзгілеу шарттарын қолдайтын пішімге түрлендіру салдарынан, ол Kaspersky Security Center (11 және одан төмен) алдыңғы нұсқаларымен үйлесімсіз болады. Сондай-ақ, түрлендірілген есепте үйлесімсіз нұсқалары бар қосалқы Басқару серверлерінен алынған деректер болмайды.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

6. **<Есеп атауы> есебін өңдеу** терезесін жабыңыз.

Өзгертілген есеп үлгісі есеп үлгілерінің тізімінде пайда болады.

Есепті файлға экспорттау

Есепті XML, HTML немесе PDF пішіміндегі файлға экспорттауға болады.

Есепті файлға экспорттау үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.

2. Файлға экспорттау қажет есеп атауының жанындағы жалаушаны қойыңыз.

3. **Есепті экспорттау** түймесін басыңыз.

4. Ашылған терезеде **Атауы** өрісінде есеп файлының атауын өзгертіңіз. Әдепкі бойынша файл атауы таңдалған есеп үлгісінің атауына сай келеді.

5. Есеп файлының түрін таңдаңыз: XML, HTML немесе PDF.

6. **Есепті экспорттау** түймесін басыңыз.

   Есеп таңдалған пішімде, әдепкі қалтаға, сіздің құрылғыңызға жүктеледі немесе сіз файлды қажетті жерге сақтай алуыңыз үшін, браузеріңізде **Басқаша сақтау** стандартты терезесі ашылады.

Есеп файлға сақталады.

Есепті жасау және қарау

Есепті жасау және қарау үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.

2. Есепті жасау үшін пайдаланғыңыз келетін есеп үлгісінің атауын басыңыз.

Жасалған есеп таңдалған үлгіні пайдаланып көрсетіледі.

Есеп деректері Басқару серверінің локализация тіліне сәйкес көрсетіледі.

Есепте келесі деректер көрсетіледі:

- **Жиынтық ақпарат** қойыншасында:
  - Есептің түрі мен атауы, оның қысқаша сипаттамасы мен есепті кезеңі және есептің қай құрылғылар тобы үшін жасалғаны туралы ақпарат.
  - Есептің анағұрлым тән деректері бар графикалық диаграмма.
  - Есептелетін есеп көрсеткіштері бар жиынтық кесте.
- **Мәліметтер** қойыншасында есептің егжей-тегжейлі деректері бар кесте көрсетіледі.

Есептерді жеткізу тапсырмасын жасау

Таңдалған есептерді жеткізу тапсырмасын жасауға болады.

Есептерді жеткізу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.
2. Есептерді жеткізу тапсырмасын жасағыңыз келетін есеп үлгілерінің жанына жалаушаларды қойыңыз.
3. **Жеткізу тапсырмасын жасау** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады. Шебердің жұмысын жалғастыру үшін **Келесі** түймесін басыңыз.
4. Шебердің **Жаңа тапсырма параметрлері** қадамында тапсырманың атауын енгізіңіз.

   Әдепкі тапсырма атауы — **Есептерді жеткізу.** Егер аттас тапсырма бұрыннан бар болса, тапсырма атауына сериялық нөмір қосылады (<N>).
5. Шебердің **Есеп конфигурациясы** қадамында келесі параметрлерді көрсетіңіз:
   a. Тапсырма арқылы жіберілетін есеп үлгілері.
   b. Есеп пішімі: HTML, XLS немесе PDF.

      wkhtmltopdf құралы есепті PDF пішіміне түрлендіру үшін қажет. PDF параметрі таңдалғанда, Басқару сервері wkhtmltopdf утилитасы құрылғыда орнатылғанын тексереді. Құрал орнатылмаған болса, бағдарлама оны Басқару серверінде орнату қажет екендігі туралы хабарламаны көрсетеді. Құралды қолмен орнатып, келесі қадамға өтіңіз.
   c. Есептер электрондық пошта арқылы жіберіле ме, сондай-ақ пошта хабарландыруларының параметрлері.

      Сіз ең көбі 20 электрондық пошта мекенжайын енгізе аласыз. Электрондық пошта мекенжайларын бөлу үшін **Enter** пернесін басыңыз. Сондай-ақ, үтірмен бөлінген электрондық пошта мекенжайларының тізімін қойып, **Enter** пернесін бассаңыз да болады.
   d. Есептер қалтаға сақталады ма, сол қалтада бұрын сақталған есептер қайта жазыла ма және қалтаға қатынасу үшін бөлек есептік жазба қолданыла ма (ортақ қатынасы бар қалта үшін).
6. Шебердің **Тапсырма кестесін конфигурациялау** қадамында тапсырманы іске қосу кестесін таңдаңыз.

Тапсырманы іске қосу кестесінің келесі нұсқалары қолжетімді:

- **Қолмен**

  Тапсырма автоматты түрде іске қосылмайды. Тапсырманы тек қолмен іске қосуға болады.

  Әдепкі бойынша, осы нұсқа таңдалған.

- **N минут сайын**

  Тапсырма жүйелі түрде, тапсырма жасалған күні көрсетілген уақыттан бастап, минуттар түрінде белгіленген аралықпен орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік уақыттан бастап 30 минут сайын іске қосылады.

- **N сағат сайын**

  Тапсырма көрсетілген күн мен уақыттан бастап, сағат түрінде белгіленген аралықпен жүйелі түрде орындалады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап 6 сағат сайын іске қосылып тұрады.

- **N күн сайын**

  Тапсырма, күндер түрінде белгіленген аралықпен жүйелі түрде орындалады. Сондай-ақ, сіз тапсырманы бірінші рет іске қосу күні мен уақытын да көрсете аласыз. Бұл қосымша параметрлерге сіз тапсырма жасап жатқан бағдарлама қолдау көрсетсе, олар қолжетімді болады.

  Әдепкі бойынша, тапсырма ағымдағы жүйелік күн мен уақыттан бастап күн сайын іске қосылады.

- **N апта сайын**

  Тапсырма жүйелі түрде, апта түрінде белгіленген аралықпен, аптаның көрсетілген күнінде және көрсетілген уақытта орындалады.

  Әдепкі бойынша, тапсырма дүйсенбі сайын, ағымдағы жүйелік уақытта іске қосылады.

- **Ай сайын**

  Тапсырма жүйелі түрде, айдың көрсетілген күнінде, көрсетілген уақытта орындалады.

  Көрсетілген күні жоқ айларда тапсырма соңғы күні орындалады.

  Әдепкі бойынша, тапсырма әр айдың бірінші күнінде, ағымдағы жүйелік уақытта орындалады.

- **Белгіленген күндері**

  Тапсырма жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, басталу уақыты 18:00 және айдың күндері таңдалмайды.

  > Айдағы нақты күнді де, апта нөмірін де (айдың бірінші, екінші аптасын) емес, ай ішіндегі апта күнінің реттік нөмірін таңдайтыныңызды ескеріңіз. Мысалы, егер сіз курсорды **Сс** жолдың **Бірінші** ұяшығына орнатсаңыз, бұл тапсырма әр жаңа айдың бірінші сейсенбісінде орындалатынын білдіреді.

  Аптаның бірнеше күнін таңдай аласыз.

- **Вирустық шабуылды анықтағанда**

  Тапсырманы *Вирустық шабуыл* оқиғасы туындағаннан кейін іске қосуға болады. Вирустық шабуылдарды қадағалайтын бағдарлама түрлерін таңдаңыз. Бағдарламалардың келесі түрлері қолжетімді:

  - жұмыс станциялары мен файлдық серверлерге арналған вирусқа қарсы бағдарламалар;
  - периметрлік қорғанысқа арналған вирусқа қарсы бағдарламалар;
  - пошталық жүйелерге арналған вирусқа қарсы бағдарламалар.

  Әдепкі бойынша, бағдарламалардың барлық түрлері таңдалған.

  Вирустық шабуыл туралы хабарлайтын қауіпсіздік бағдарламасының түріне байланысты әртүрлі тапсырмаларды іске қосуға болады. Бұл жағдайда, сізге қажет емес бағдарлама түрлерін таңдауды алып тастаңыз.

- **Басқа тапсырманы аяқтағанда**

  Ағымдағы тапсырма басқа тапсырма аяқталғаннан кейін іске қосылады. Екі тапсырма да бір құрылғы арқылы тағайындалса ғана, осы параметр жұмыс істейді. Мысалы, *Құрылғыларды басқару* тапсырмасын **Құрылғыны қосу** параметрінің көмегімен іске қоса аласыз және ол аяқталғаннан кейін *Вирустарды іздеу* тапсырмасын іске қоса аласыз.

  Кестеден іске қосу тапсырмасын және осы тапсырма орындалатын күйді таңдау керек (**Сәтті аяқталды** немесе **Сәтсіз аяқталды**).

  Қажет болса, кестедегі тапсырмаларды төмендегідей іздеуге, сұрыптауға және сүзуге болады:

  - Тапсырманы атауы бойынша іздеу үшін іздеу өрісіне тапсырма атауын енгізіңіз.
  - Тапсырмаларды атауы бойынша сұрыптау үшін сұрыптау белгішесін басыңыз.

    Әдепкі бойынша, тапсырмалар өсу ретімен әліпбилік ретпен сұрыпталады.
  - Сүзгі белгішесін басыңыз және ашылатын терезеде тапсырмаларды топтар бойынша сүзіңіз, содан кейін **Қолдану** түймесін басыңыз.

7. Шебердің осы қадамында тапсырманы іске қосу кестесінің басқа параметрлерін конфигурациялаңыз:

- **Тапсырма кестесі** бөлімінде бұрын таңдалған кестені тексеріңіз немесе қайта конфигурациялаңыз және кезеңді, ай немесе апта күндерін орнатыңыз, вирус шабуылының шартын немесе тапсырманы іске қосу ретінде басқа тапсырманың орындалуын белгілеңіз. Бұл бөлімде қолайлы кесте таңдалған болса, басталу уақытын да көрсетуге болады.
- **Қосымша параметрлер** бөлімінде келесі параметрлерді көрсетіңіз:

  - **Өткізіп алынған тапсырмаларды іске қосу**

    Бұл параметр, тапсырма басталғалы тұрған кезде клиент құрылғысы желіде көрсетілмесе, тапсырманың жүріс-тұрысын анықтайды.

    Параметр қосулы болса, клиент құрылғысында Kaspersky бағдарламасын кезекті рет іске қосу кезінде тапсырманы іске қосу әрекеті жасалады. Тапсырманың кестесінде **Қолмен**, **Бір рет** немесе **Дереу** іске қосу көрсетілсе, онда тапсырма желіде құрылғы көзге көрінетін болғаннан кейін немесе құрылғы тапсырманың әрекет ету ауқымына қосылғаннан кейін бірден іске қосылады.

    Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу тек кесте бойынша орындалатын болады. **Қолмен**, **Бір рет** және **Дереу** кестесі үшін тапсырмалар желіде көрінетін клиенттік құрылғыларда ғана орындалады. Мысалы, сіз бұл параметрді тек жұмыс уақытынан тыс уақытта іске қосқыңыз келетін ресурстарды қажетсінетін тапсырма үшін өшіре аласыз.

Әдепкі бойынша, параметр өшірулі.

- **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады, яғни *тапсырманың таратылған іске қосылуы* орын алады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Таратылған іске қосылу кезеңі, тапсырма тағайындалған клиент құрылғыларының санына байланысты тапсырманы жасау кезінде автоматты түрде есептеледі. Кейінірек, тапсырма әрқашан есептелген іске қосу уақытында іске қосылады. Алайда, тапсырма параметрлеріне түзетулер енгізілгенде немесе тапсырма қолмен іске қосылғанда, тапсырманы іске қосу уақытының есептелген мәні өзгереді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

- **Тапсырманы бастауға арналған келесі аралықтағы автоматты кездейсоқ кідірісті пайдалану**

  Параметр қосулы болса, тапсырма клиент құрылғыларында белгілі бір уақыт аралығында кездейсоқ іске қосылады. Тапсырманың таратылған іске қосылуы, тапсырманы кесте бойынша іске қосу кезінде көптеген клиент құрылғыларының Басқару серверіне бір уақытта жүгінуіне жол бермейді.

  Егер параметр өшірулі болса, клиент құрылғыларында тапсырманы іске қосу кесте бойынша орындалады.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша, уақыт аралығы бір минутқа тең.

- **Тапсырма мынанша уақыттан көбірек орындалып жатса, оны тоқтату**

  Белгіленген уақыттан кейін, тапсырма аяқталғанына немесе аяқталмағанына қарамастан автоматты түрде тоқтатылады.

  Егер сіз тым ұзақ орындалатын тапсырмаларды үзгіңіз келсе (немесе тоқтатқыңыз келсе), осы параметрді қосыңыз.

  Әдепкі бойынша, параметр өшірулі. Әдепкі бойынша тапсырманы орындау уақыты – 120 минут.

8. Шебердің **Тапсырманы іске қосу үшін есептік жазбаны таңдау** қадамында тапсырманы іске қосу үшін пайдаланылатын есептік жазба деректерін көрсетіңіз.

9. Тапсырманы жасағаннан кейін, оның басқа параметрлерін өзгерту қажет болса, шебердегі **Тапсырманы жасауды аяқтау** қадамында **Жасап болған соң, тапсырма туралы мәліметтерді ашу** опциясын қосыңыз (әдепкісінше бұл опция қосулы болады).

10. Тапсырма жасау және шеберді жабу үшін **Аяқтау** түймесін басыңыз.

    Есепті жіберу тапсырмасы жасалады. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрі қосылса, тапсырма параметрлері терезесі ашылады.

Есеп үлгілерін жою

Есеп үлгілерін жою үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Есептер** бөліміне өтіңіз.

2. Жойғыңыз келетін есеп үлгілеріне қарсы жалаушаларды қойыңыз.

3. **Жою** түймесін басыңыз.

4. Пайда болған терезеде таңдауыңызды растау үшін **ОК** түймесін басыңыз.

Таңдалған есеп үлгілері жойылады. Егер бұл есеп үлгілері есептерді жіберу тапсырмаларына енгізілген болса, олар да осы тапсырмалардан жойылады.

Оқиғалар және оқиғаларды таңдау

Бұл бөлімде оқиғалар мен оқиғалар таңдау, Kaspersky Security Center құрамдастарында орын алған оқиғалар түрлері және жиі болатын оқиғаларды бұғаттауды басқару туралы ақпарат бар.

Kaspersky Security Center-дегі оқиғалар туралы

Kaspersky Security Center бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады.

Оқиға түрлері

Kaspersky Security Center-де хабарландырулардың келесі түрлері бар:

- Жалпы оқиғалар. Бұл оқиғалар барлық Kaspersky басқарылатын бағдарламаларында туындайды. Мысалы, Вирустық шабуыл жалпы оқиға. Жалпы оқиғалар қатаң белгіленген синтаксис пен семантикаға ие. Жалпы оқиғалар, мысалы, есептер мен мониторинг тақтасында қолданылады.

- Kaspersky басқарылатын бағдарламаларының айрықша оқиғалары. Kaspersky әрбір басқарылатын бағдарламасы өзіндік оқиғалар жиынтығына ие.

Оқиғалар көздері

Оқиғалар келесі бағдарламалар тарапынан жасалуы мүмкін:

- Kaspersky Security Center бағдарламасының құрамдастары:
  - Басқару сервері
  - Желілік агент
  - iOS MDM сервері
  - Exchange ActiveSync ұялы құрылғылар сервері
- Kaspersky басқарылатын бағдарламалары

  Kaspersky басқарылатын қолданбалары жасайтын оқиғалар туралы қосымша ақпарат тиісті қолданба құжаттамасында келтірілген.

Қолданба жасай алатын оқиғалардың толық тізімі қолданба саясатындағы **Оқиғаларды конфигурациялау** қойындысында келтірілген. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға болады.

Оқиғаның маңыздылық деңгейі

Әрбір оқиғаның өзіндік маңыздылық деңгейі бар. Туындау шарттарына байланысты, оқиғаға түрлі маңыздылық деңгейлері белгіленуі мүмкін. Оқиғалар маңыздылығының төрт деңгейі бар:

- *Критикалық оқиға* – деректерді жоғалтуға, жұмыстағы ақауға немесе критикалық қатеге әкелуі мүмкін критикалық мәселенің туындағанын білдіретін оқиға.
- *Функционалдық ақау* – бағдарламаның жұмысы немесе рәсімді орындау барысында туындаған күрделі мәселенің, қатенің немесе ақаудың орын алғанын білдіретін оқиға.
- *Ескерту* – міндетті түрде күрделі болып саналмаса да, болашақта мәселенің туындауы мүмкін екенін білдіретін оқиға. Оқиғалар туындағаннан кейін бағдарламаның жұмысы деректерді немесе функционалдық мүмкіндіктерді жоғалтпай қалпына келтіріле алса, осы оқиғалар көбінесе Ескертулерге қатысты болып келеді.
- *Ақпараттық хабарлар* – операцияның сәтті орындалуы, бағдарламаның дұрыс жұмыс істеуі немесе рәсімнің аяқталуы туралы хабарлау мақсатында туындайтын оқиға.

Әрбір оқиға үшін Kaspersky Security Center-де қарап шығуға немесе өзгертуге болатын сақтау уақыты белгіленген. Кейбір оқиғалар Басқару серверінің дерекқорында әдепкі бойынша сақталмайды, себебі олар үшін белгіленген уақыт нөлге тең. Сыртқы жүйелерге, Басқару серверінің дерекқорында кемінде бір күн бойы сақталатын оқиғалар ғана экспортталуы мүмкін.

Оқиға таңдауларын пайдалану

Оқиғаларды таңдау, экранда Басқару серверінің дерекқорынан таңдалған аталған оқиғалар жиынтығын көруге арналған. Осы оқиға түрлері келесі санаттар бойынша топтастырылған:

- Маңыздылық деңгейі: **Критикалық оқиғалар**, **Функциялық ақаулар**, **Ескертулер** және **Ақпараттық оқиғалар**.
- Уақыт: **Соңғы оқиғалар**.
- Түрі: **Пайдаланушылардың сұраулары** және **Аудит оқиғалары**.

Kaspersky Security Center Web Console интерфейсінде конфигурациялауға қолжетімді параметрлер негізінде пайдаланушы тарапынан айқындалған оқиғалар таңдауын жасай аласыз және көре аласыз.

Оқиғаларды таңдау Kaspersky Security Center Web Console бағдарламасының **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөлімінде қолжетімді.

Әдепкі бойынша, оқиғаларды таңдау соңғы жеті күн ішіндегі ақпаратты қамтиды.

Kaspersky Security Center бағдарламасында әдепкі бойынша таңдаулар жиынтығы бар (алдын ала анықталған):

- Маңыздылық деңгейі әртүрлі оқиғалар:
  - **Критикалық оқиғалар**
  - **Функционалдық ақау**
  - **Ескертулер**
  - **Ақпараттық оқиғалар**
- **Пайдаланушылардың сұраулары** (басқарылатын бағдарлама оқиғалары)
- **Соңғы оқиғалар** (соңғы апта ішінде)
- **Аудит оқиғасы**.

Сондай-ақ, сіз қосымша оқиғалардың пайдаланушы таңдауларын жасап, конфигурациялай аласыз. Пайдаланушының таңдауларында, сіз оқиғаларды туындаған құрылғылар сипаттары (құрылғылар атауы, IP ауқымдары және басқару топтары) бойынша, оқиғалар түрлері және маңыздылық деңгейлері бойынша, бағдарлама мен құрамдастың атауы бойынша, сондай-ақ уақыт аралығы бойынша сүзгілей аласыз. Сондай-ақ, тапсырма нәтижелерін іздеу аймағына қосуға болады. Сонымен қатар, сөзді немесе бірнеше сөзді енгізуге болатын іздеу өрісін де қолдануға болады. Кез келген енгізілген сөздерді олардың сипаттарының (оқиға атауы, сипаттама, құрамдас атауы сияқты) кез келген жерінде қамтитын барлық оқиғалар көрсетіледі.

Алдын ала анықталған таңдаулар үшін де, пайдаланушы таңдаулары үшін де, көрсетілетін оқиғалардың санын немесе ізделетін жазбалар санын шектеуге болады. Екі нұсқа да Kaspersky Security Center оқиғаларды көрсететін уақытқа әсер етеді. Дерекқор неғұрлым үлкен болса, процесс соғұрлым көп уақытты қажет етеді.

Сіз келесіні орындай аласыз:

- Оқиғаны таңдау параметрлерін өзгерту.
- Оқиғалар таңдауын жасау.
- Таңдалған оқиғалар таңдауы туралы мәліметті көру.
- Оқиғалар таңдауын жою.
- Басқару сервері дерекқорынан оқиғаларды жою.

Оқиғалар таңдауын жасау

Оқиғалар таңдауын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.
3. Ашылған **Жаңа оқиғаны таңдау** терезесінде жаңа оқиғалар таңдауы параметрлерін көрсетіңіз. Параметрлерді осы терезенің бірнеше бөлімдерінде көрсетуге болады.

4. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

   Растау терезесі ашылады.

5. Оқиғаларды таңдаудың нәтижелерін қарау үшін **Таңдау нәтижесіне өту** жалаушасын қойыңыз.

6. Оқиғалар таңдауын жасауды растау үшін **Сақтау** түймесін басыңыз.

Таңдау нәтижесіне өту жалаушасы қойылған болса, оқиғалар таңдауы нәтижесі экранда көрсетіледі. Әйтпесе, жаңа оқиғалар таңдауы оқиғалар таңдауы тізімінде пайда болады.

Оқиғалар таңдауын өзгерту

Оқиғалар таңдауын өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Өзгертуді қажет ететін оқиғалар таңдауына қарама-қарсы жалаушаны қойыңыз.

3. **Сипаттар** түймесін басыңыз.

   Оқиғалар таңдауы сипаттары терезесі ашылады.

4. Оқиғалар таңдауы сипаттарын өңдеңіз.

   > Алдын ала анықталған оқиғалар таңдауы үшін сипаттарды тек келесі қойыншаларда өңдеуге болады: **Жалпы** (таңдау атауын қоспағанда), **Уақыт** және **Қатынасу құқықтары**.

   Пайдаланушы таңдаулары үшін барлық сипаттарды өңдеуге болады.

5. Өзгерістерін сақтау үшін **Сақтау** түймесін басыңыз.

Өзгертілген оқиғалар таңдауы тізімде көрсетіледі.

Оқиғалар таңдауы тізімін қарау

Оқиғалар таңдауын қарап шығу:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Іске қосу қажет оқиғалар таңдауына қарама-қарсы жалаушаны қойыңыз.

3. Келесі әрекеттердің бірін орындаңыз:

   - Оқиғалар таңдауы нәтижелері үшін сұрыптауды конфигурациялау үшін:

     a. **Сұрыптауды қайта конфигурациялау және іске қосу** түймесін басыңыз.

     b. Пайда болған **Оқиғаны таңдау үшін сұрыптауды қайта конфигурациялау** терезесінде сұрыптау параметрлерін көрсетіңіз.

     c. Таңдаудың атауын басыңыз.

   - Әйтпесе, оқиғалар тізімін Басқару серверінде сақталғандай етіп көргіңіз келсе, таңдаудың атауын басыңыз.

Оқиғалар таңдауы нәтижесі көрсетіледі.

Оқиғалар таңдауын экспорттау

Kaspersky Security Center қолданбасы оқиғалар таңдауын және оның параметрлерін KLO файлына сақтауға мүмкіндік береді. Сақталған оқиға таңдауын Kaspersky Security Center Windows, сондай-ақ Kaspersky Security Center Linux жүйелеріне импорттау үшін KLO файлын пайдалануға болады.

Пайдаланушы анықтаған оқиға таңдауларының кейбіреуін ғана жоюға болатынын ескеріңіз. Kaspersky Security Center жүйесінде әдепкі бойынша орнатылған оқиға таңдауларының жиынын (алдын ала анықталған таңдаулар) файлға сақтау мүмкін емес.

Оқиғалар таңдауын экспорттау үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру** → **Оқиғаларды таңдау** бөліміне өтіңіз.

2. Экспорттау қажет оқиғалар таңдауына қарама-қарсы жалаушаны белгілеңіз.

   Бірнеше оқиға таңдауын бір уақытта экспорттау мүмкін емес. Бірнеше таңдауды таңдасаңыз, **Экспорттау** түймесі өшірулі болады.

3. **Экспорттау** түймесін басыңыз.

4. Ашылған **Басқаша сақтау** терезесінде оқиғалар таңдауы файлының атын және жолын көрсетіңіз, содан кейін **Сақтау** түймесін басыңыз.

   Басқаша сақтау терезесі Google Chrome, Microsoft Edge немесе Opera қолдансаңыз ғана көрсетіледі. Басқа браузерді қолдансаңыз, оқиғалар таңдауының файлы **Жүктеп алынғандар** қалтасына автоматты түрде сақталады.

Оқиғалар таңдауын импорттау

Kaspersky Security Center жүйесі оқиғалар таңдауын KLO файлынан импорттауға мүмкіндік береді. KLO файлы экспортталған оқиғалар таңдауын және оның параметрлерін қамтиды.

Оқиғалар таңдауын импорттау үшін:

1. Қолданбаның негізгі терезесінде **Бақылау және есеп беру → Оқиғаларды таңдау** бөліміне өтіңіз.
2. Импорттағыңыз келетін оқиғалар таңдауы файлын таңдау үшін **Импорттау** түймесін басыңыз.
3. Ашылған терезеде KLO саясаты файлына апаратын жолды көрсетіңіз және **Ашу** түймесін басыңыз. Назар аударыңыз: оқиғалар таңдауының тек бір файлын таңдауға болады.

   Оқиғалар таңдауын өңдеу басталады.

Импорт нәтижелері бар хабарландыру пайда болады. Оқиғалар таңдауы импортталса, таңдау сипаттарын көру үшін **Импорттау мәліметтерін көру** сілтемесін басуға болады.

Сәтті импорттаудан кейін оқиғалар таңдауы таңдау тізімінде пайда болады. Оқиғалар таңдауының параметрлері де импортталады.

Импортталған жаңа оқиғалар таңдауының атауы бұрыннан бар таңдау атауымен бірдей болса, импортталған таңдау атауы түр **(<реттік нөмір>)**, мысалы: **(1)**, **(2)** жалғауы көмегімен кеңейтіледі.

Оқиға туралы ақпаратты көру

Оқиға туралы ақпаратты көру үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаға басыңыз.

   Оқиғаның сипаттары терезесі ашылады.
3. Ашылған терезеде келесі әрекеттерді орындауға болады:
   - Таңдалған оқиғаның ақпаратын қарау.
   - Тізімдегі келесі немесе алдыңғы оқиғаға өту — оқиғаларды таңдаудың нәтижелері.
   - Оқиға туындаған құрылғыға өту.
   - Оқиға туындаған құрылғыны қамтитын басқару тобына өту.
   - Тапсырмамен байланысты оқиға үшін тапсырманың сипаттарына өтіңіз.

Оқиғаларды файлға экспорттау

Kaspersky Security Center оқиғаларды оқиға таңдауынан TXT файлына сақтауға мүмкіндік береді.

Оқиғаларды файлға экспорттау үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаның жанындағы жалаушаны қойыңыз.

   Сондай-ақ бірнеше оқиғаны немесе бүкіл оқиғаны таңдауға болады.
3. **Файлға экспорттау** түймесін басыңыз.

Таңдалған оқиға TXT файлына экспортталады.

Оқиғадан нысан тарихын қарау

Тексеруді басқаруды қолдайтын нысанды жасау оқиғасынан немесе өзгерту оқиғасынан нысанды тексеру тарихына өтуге болады.

Оқиғадан нысанның тарихын көру үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғаның жанындағы жалаушаны қойыңыз.
3. **Тексерістер журналы** түймесін басыңыз.

Нысанды тексеру тарихы ашылады.

Оқиғаларды жою

Бір немесе бірнеше оқиғаны жою үшін:

1. Оқиғалар таңдауын іске қосыңыз.
2. Қажетті оқиғалардың жанында жалаушаларды қойыңыз.
3. **Жою** түймесін басыңыз.

Таңдалған оқиғалар жойылды және оларды қалпына келтіру мүмкін емес.

Оқиға таңдауларын жою

Пайдаланушылардың оқиғалар таңдауын ғана жоюға болады. Алдын ала анықталған оқиғалар таңдауын жоюға болмайды.

Оқиғалар таңдауын жою үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру → Оқиғаларды таңдау** бөліміне өтіңіз.
2. Жойғыңыз келетін оқиғалар таңдауына қарсы жалаушаларды қойыңыз.
3. **Жою** түймесін басыңыз.
4. Пайда болған терезеде **OK** түймесін басыңыз.

Оқиғалар таңдауы жойылады.

Оқиғаны сақтау мерзімін конфигурациялау

Kaspersky Security Center бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады. Кейбір оқиғаларды әдепкі бойынша көрсетілгеннен әлдеқайда ұзақ немесе қысқа мерзімде сақтау қажет болуы мүмкін. Оқиғаның әдепкі бойынша сақтау мерзімін өзгертуге болады.

Басқару сервері дерекқорында қандай да бір оқиғаларды сақтауға қызығушылық танытпасаңыз, Басқару сервері саясатында, Kaspersky бағдарламасы саясатында немесе Басқару сервері сипаттарында (тек Басқару сервері оқиғалары үшін) тиісті параметрді өшіре аласыз. Бұл дерекқордағы оқиғалар түрлерінің санын азайтады.

Оқиғаны сақтау мерзімі неғұрлым ұзақ болса, дерекқор максималды өлшемге соғұрлым тез жетеді. Алайда, оқиғаны барынша ұзақ сақтау мерзімі мониторинг тапсырмаларын орындауға және есептерді аса ұзақ кезең бойы қарауға мүмкіндік береді.

Басқару сервері дерекқорында оқиғаны сақтау мерзімін белгілеу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар) → Саясаттар және профильдер** бөліміне өтіңіз.
2. Қажетті саясаттың атауын басыңыз.

   Басқарылатын Kaspersky қолданбасының, желілік агенттің немесе басқару серверінің саясатын таңдауға болады. Қажетті басқару серверінің жанындағы параметрлер белгішесін ( ) басу арқылы оқиғаларды сақтау шартын конфигурациялауға да болады.
3. **Оқиғаларды конфигурациялау** қойыншасын таңдаңыз.

   Байланысты оқиғалар тізімі бар **Критикалық** бөлімі көрсетіледі. Қажет болса, **Функционалдық ақау**, **Ескерту** немесе **Ақпараттық** бөліміне өтуге болады.
4. Оң жақ тақтадағы оқиғалар түрлерінің тізімінде сақтау мерзімін өзгерткіңіз келетін оқиға атауының сілтемесіне өтіңіз.

   Ашылған терезенің **Оқиғаларды тіркеу** бөлімінде **Басқару серверінің дерекқорында сақтау мерзімі (күндер)** ауыстырғыш түймесі қосылады.
5. Қосқыштың астындағы өңдеу өрісінде оқиғаны сақтау күндерінің санын көрсетіңіз.

6. Оқиғаны Басқару сервері дерекқорында сақтағыңыз келмесе, **Басқару серверінің дерекқорында сақтау мерзімі (күндер)** параметрін өшіріңіз.

   Басқару сервері оқиғаларын Басқару сервері сипаттары терезесінде конфигурацияласаңыз және оқиға параметрлері Kaspersky Security Center Басқару сервері саясатында бұғатталған болса, оқиғаны сақтау мерзімінің мәнін өзгерте алмайсыз.

7. **ОК** түймесін басыңыз, содан кейін оң жақ тақта жабылғаннан кейін, **Сақтау** түймесін басыңыз.

   Саясат сипаттары терезесі жабылады.

Енді Басқару сервері таңдалған түрдегі оқиғаларды қабылдап, сақтаған кезде, олардың сақтау мерзімі өзгертіледі. Басқару сервері бұрын алынған оқиғаларды сақтау мерзімін өзгертпейді.

Kaspersky Security Center құрамдастарының оқиғалары

Kaspersky Security Center әрбір құрамдасының өзіндік оқиғалар түрлерінің жиынтығы бар. Бұл бөлімде Kaspersky Security Center басқару серверінде, желілік агентте және iOS MDM серверінде орын алатын оқиғалардың түрлері берілген. Kaspersky бағдарламаларында орын алатын оқиғалар түрлері бұл бөлімде атап көрсетілмеген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрі сипаттамасы деректерінің құрылымы

Оқиғалардың әр түрі үшін оның аты, идентификаторы, әріптік коды, сипаттамасы және әдепкі бойынша сақтау уақыты көрсетіледі.

- **Оқиға түрінің көрсетілетін атауы**. Бұл мәтін Kaspersky Security Center бағдарламасында оқиғаларды орнатқан кезде және олар пайда болған кезде көрсетіледі.
- **Оқиға түрі идентификаторы**. Бұл сандық код үшінші тарап оқиғаларын талдау құралдарын қолдана отырып, оқиғаларды өңдеуде қолданылады.
- **Оқиға түрі** (әріптік код). Бұл код Kaspersky Security Center дерекқорының жария көріністерін пайдалана отырып, оқиғаларды қарау және өңдеу кезінде және оқиғаларды SIEM жүйелеріне экспорттау кезінде пайдаланылады.
- **Сипаттамасы**. Бұл мәтінде оқиға болған кездегі жағдайдың сипаттамасы және бұл жағдайда не істеуге болатыны туралы сипаттама келтірілген.
- **Әдепкі бойынша сақтау мерзімі**. Бұл, оқиға Басқару серверінің дерекқорында сақталатын және Басқару сервері оқиғаларының тізімінде көрсетілетін күндер саны. Осы кезең аяқталғаннан кейін, оқиға жойылады. Егер оқиғаны сақтау уақытының мәні 0 болып көрсетілсе, мұндай оқиғалар тіркеледі, бірақ Басқару сервері оқиғалары тізімінде көрсетілмейді. Егер сіз осындай оқиғаларды операциялық жүйенің оқиғалар журналында сақтауды конфигурациялаған болсаңыз, оларды сол жерден таба аласыз.

Оқиғаларды сақтау уақытын өзгертуге болады:

- Басқару консолі: Оқиғаны сақтау мерзімін конфигурациялау.
- Kaspersky Security Center Web Console: Оқиғаны сақтау мерзімін конфигурациялау.

Басқа деректер келесі өрістерді қамтуы мүмкін:

- **event_id**: дерекқордағы оқиғаның автоматты түрде жасалған және тағайындалған бірегей нөмірі; **Оқиға түрінің идентификаторымен** шатастырмау керек.
- **task_id**: орындау нәтижесінде оқиға туындаған тапсырма идентификаторы (ондай бар болса).
- **severity**: келесі маңыздылық деңгейлерінің бірі (маңыздылықтың өсуі ретімен):

  0) Жол бергісіз маңыздылық деңгейі.

  1) Ақпараттық.

  2) Ескерту.

  3) Қате.

  4) Критикалық.

Басқару сервері оқиғалары

Бұл бөлімде Басқару сервері оқиғалары туралы ақпарат бар.

Басқару серверінің критикалық оқиғалары

Төмендегі кестеде **Критикалық** маңыздылық деңгейі бар Kaspersky Security Center Басқару сервері оқиғаларының түрлері келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару консолиндегі басқару серверінің сипаттары терезесінде портты көрсетсеңіз, **Kaspersky Security Center қызметі** Promtheus (бақылау және ескерту жүйесі) қабылдайтын оның көрсеткіштері мен критикалық оқиғаларын жариялайды. Prometheus көрсеткіштерді және критикалық оқиғаларды алады, содан кейін әрбір оқиға үшін ескертулер жасайды.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Басқару серверінің критикалық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензиялық шектеу асырылды	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Күніне бір рет Kaspersky Security Center бағдарламасы лицензиялық шектеудің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын лицензиялық бірліктердің жалпы санының 110%-нан асса туындайды. Осы оқиға туындаса да, клиент құрылғылары қорғалған. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Вирустық шабуыл	26 (Файл қауіптерінен қорғаныс құрамдасы үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	180 күн
Вирустық шабуыл	27 (Пошта қауіптерінен қорғаныс құрамдасы үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	180 күн
Вирустық шабуыл	28 (желілік экран үшін)	GNRL_EV_VIRUS_OUTBREAK	Осы түрдегі оқиғалар, бірнеше басқарылатын құрылғыда қысқа кезең ішінде анықталған зиянды нысандардың саны белгіленген шекті мәндерден асып кетсе туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің сипаттарында шекті мәндерді конфигурациялаңыз. • Белсендірілетін аса қатаң саясатты жасаңыз немесе осы оқиға туындаған кезде іске қосылатын тапсырманы жасаңыз.	180 күн
Құрылғы басқарылмайтын күйге айналды	4111	KLSRV_HOST_OUT_CONTROL	Осы түрдегі оқиғалар, басқарылатын құрылғы желіде көрініп тұрса да, Басқару сервері белгіленген кезең ішінде қосылмаған жағдайда туындайды. Құрылғыда Желілік агенттің дұрыс жұмыс істеуіне не кедергі келтіретінін анықтаңыз. Ықтимал себептеріне желі ақаулары және құрылғыдан Желілік агентті жою кіруі мүмкін.	180 күн
Құрылғының күйі: "Критикалық"	4113	KLSRV_HOST_STATUS_CRITICAL	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Критикалық* күйі тағайындалса туындайды. Сіз шарттарды конфигурациялай аласыз, оларды орындау кезінде құрылғының күйі *Критикалық* болып өзгереді.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Кілт файлы қара тізімге қосылды	4124	KLSRV_LICENSE_BLACKLISTED	Осы түрдегі оқиғалар, Kaspersky бағдарламасы сіз қолданып жатқан белсендіру кодын немесе лицензиялық кілтті тыйым салынғандар тізіміне қосқан болса туындайды. Толығырақ ақпарат алу үшін Техникалық қолдау қызметіне жүгініңіз.	180 күн
Шектелген функционалдылық режимі	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Осы түрдегі оқиғалар, Kaspersky Security Center бағдарламасы Ұялы құрылғыларды басқару және Осалдықтар мен патчтарды басқару мүмкіндігінің қолдауынсыз, базалық функционалдылық режимінде жұмыс істей бастаса туындайды. Төменде себептер және оқиғаға берілген тиісті жауаптар келтірілген: • Лицензия мерзімі өтті. Kaspersky Security Center толық функционалдылығына лицензия беріңіз (Басқару серверіне белсендіру кодын немесе кілт файлын қосыңыз). • Басқару сервері ұсынылған лицензия бойынша қолданылуы мүмкін саннан көп құрылғылар санын басқарады. Құрылғыларды бір Сервердің басқару топтарының құрамынан басқа Сервердің басқа топтарына жылжытыңыз (басқа Сервердің лицензиялық шектеуі асып кетпесе).	180 күн
Лицензияның қолданылу мерзімі жақында аяқталады	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Осы түрдегі оқиғалар, коммерциялық лицензияның жарамдылық мерзімінің аяқталу күні жақындаса туындайды. Күніне бір рет Kaspersky Security Center бағдарламасы лицензияның лицензия мерзімінің өтпегенін тексеріп тұрады. Осы түрдегі оқиғалар 30 күн, 15 күн, 5 күн және 1 күн бұрын, лицензия мерзімі аяқталғанға дейін жарияланады. Сіз күндер санын өзгерте алмайсыз. Басқару сервері лицензияның жарамдылық мерзімінің аяқталу күніне дейін көрсетілген күні өшірілсе, оқиға келесі күнге дейін жарияланбайды. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, Kaspersky Security Center бағдарламасы Базалық функционалдылық режимінде жұмыс істейді. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Резервттегі лицензиялық кілт Басқару серверіне қосылғанына көз жеткізіңіз. • Жазылымды қолдансаңыз, оның мерзімін ұзартыңыз. Провайдерге алғы төлем уақтылы төленген болса, шектелмеген жазылым автоматты түрде ұзартылады.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Сертификаттың жарамдылық мерзімі бітті	4132	KLSRV_CERTIFICATE_EXPIRED	Бұл түрдегі оқиғалар мобильдік құрылғылардағы клиент сертификатының мерзімі аяқталғанда орын алады.	180 күн
Басқару сервері сертификатының мерзімі аяқталды.	6129	ServerCertificateExpired	Осы түрдегі оқиғалар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару сервері сертификаттарының жарамдылық мерзімі аяқталғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	180 күн
Kaspersky қолданбасының модульдеріне арналған жаңартулар қайтарылды	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Kaspersky техникалық қолдау қызметінің мамандары үзіліссіз жаңартуларды қайтарып алса (бұл жаңартулар үшін *Қайтарылған* күйі көрсетіледі); мысалы, оларды жаңа нұсқаға жаңарту қажет болса, осы түрдегі оқиғалар пайда болады. Оқиға Kaspersky Security Center патчтарына қатысты емес және Kaspersky басқарылатын бағдарлама модульдеріне жатпайды. Оқиға жаңартулардың орнатылмауы себебін қамтиды.	180 күн
Аудит: SIEM серверіне экспорттау сәтсіз аяқталды	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Осы түрдегі оқиғалар, SIEM жүйесіне оқиғаларды экспорттау SIEM жүйесіне қосылу қатесіне байланысты сәтсіз аяқталғанда орын алады.	180 күн

Басқару серверінің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center Басқару сервері оқиғаларының түрлері келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару серверінің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Орындау уақытының қатесі	4125	KLSRV_RUNTIME_ERROR	Осы түрдегі оқиғалар белгісіз мәселелерден туындайды. Көбінесе бұл ДҚБЖ мәселелері, желімен байланысты мәселелер, сондай-ақ бағдарламалық және аппараттық жасақтамамен байланысты басқа да мәселелер. Оқиға туралы толық ақпаратты оның сипаттамасынан табуға болады.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі асырылды	4126	KLSRV_INVLICPROD_EXCEDED	Басқару сервері осындай түрдегі оқиғаларды мерзімді түрде (сағат сайын) жасайды. Kaspersky Security Center бағдарламасында үшінші тарап бағдарламаларының лицензиялық кілттерін басқарсаңыз және орнату саны үшінші тарап бағдарламасының лицензиялық кілтінде белгіленген шектен асып кетсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Үшінші тарап бағдарламасын, ол қолданылмайтын құрылғылардан жойыңыз. • Үшінші тарап лицензиясын көптеген құрылғыларға қолданыңыз. Лицензиялы бағдарламалар тобының функционалдылығын қолдана отырып, лицензиялы бағдарламалардың лицензиялық кілттерін басқара аласыз. Лицензиялы бағдарламалар тобына, сіз белгілеген өлшемшарттарға сай келетін үшінші тарап бағдарламалары кіреді.	180 күн
Бұлттық сегментте сауалнаманы орындау мүмкін болмады	4143	KLSRV_KLCLOUD_SCAN_ERROR	Осы түрдегі оқиғалар, Басқару сервері бұлтты ортадағы желі сегментінде сауалнама өткізе алмаған жағдайда туындайды. Оқиғаның сипаттамасындағы ақпаратты оқып, оларға тиісінше ден қойыңыз.	Сақталмайды
Белгіленген қалтаға жаңартуларды көшіру мүмкін болмады	4123	KLSRV_UPD_REPL_FAIL	Бағдарламалық жасақтама жаңартулары ортақ қатынасы бар қалтаға (немесе қалталарға) көшірілсе, осы түрдегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Қалтаға (немесе қалталарға) қатынасу үшін пайдаланылатын пайдаланушы есептік жазбасының жазу құқығы бар-жоғын тексеріңіз. • Қалта(лар)ға арналған пайдаланушы аты және/немесе құпиясөз өзгергенін тексеріңіз. • Интернет қосылымын тексеріңіз, себебі бұл оқиғаның себебі болуы мүмкін. Дерекқорлар мен бағдарламалық модульдерді жаңарту жөніндегі нұсқауларды орындаңыз.	180 күн
Дискіде бос орын жоқ	4107	KLSRV_DISK_FULL	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғының қатты дискісінде диск кеңістігі таусылып бара жатқан жағдайда туындайды. Құрылғыдағы диск кеңістігін босатыңыз.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Ортақ қалта қолжетімсіз	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Осы түрдегі оқиғалар, Басқару серверінің ортақ қатынасы бар қалтасы қолжетімді болмағанда туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің (ортақ қатынасы бар қалта орналасқан) қосулы және қолжетімді екеніне көз жеткізіңіз. • Қалтаға арналған пайдаланушы аты және/немесе құпиясөз өзгертілгенін тексеріңіз. • Желі қосылымын тексеріңіз.	180 күн
Басқару серверінің дерекқоры қолжетімсіз	4109	KLSRV_DATABASE_UNAVAILABLE	Осы түрдегі оқиғалар Басқару сервері дерекқоры қолжетімсіз болған жағдайда пайда болады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • SQL сервері орнатылған қашықтағы сервердің қолжетімді ме екенін тексеріңіз. • ДҚБЖ оқиғалар журналдарын қарап шығыңыз және Басқару сервері дерекқорының қолжетімсіздігінің себебін табыңыз. Мысалы, алдын алу жұмыстарына байланысты, SQL Server сервері орнатылған қашықтағы сервер қолжетімді болмауы мүмкін.	180 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Басқару серверінің дерекқорында бос орын жоқ	4110	KLSRV_DATABASE_FULL	Бұл түрдегі оқиғалар Басқару сервері дерекқорында бос орын болмаса пайда болады. Басқару серверінің дерекқоры толып кетсе және дерекқорға одан әрі жазу мүмкін болмаса, Басқару сервері жұмыс істемейді. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиғаға ден қоюдың тиісті тәсілдері келтірілген: • Сіз SQL Server Express Edition қолданасыз: SQL Server Express құжаттамасында, қолданылатын нұсқа үшін дерекқор өлшеміне қойылған шектеуді тексеріңіз. Басқару серверіңіздің дерекқоры дерекқор өлшемінің шегінен асып кеткен болса керек. Басқару серверінің дерекқорында сақталатын оқиғалар санын шектеңіз. Басқару сервері дерекқорында бағдарламаларды басқару құрамдасы жіберген оқиғалар өте көп. Басқару серверінің дерекқорында Бағдарламаларды басқару құрамдасының оқиғаларын сақтауға қатысты Kaspersky Endpoint Security for Windows саясатының параметрлерін өзгертуге болады. • SQL Server Express Edition жүйесінен ерекшеленетін ДҚБЖ қолданасаңыз: Басқару серверінің дерекқорында сақталатын оқиғалар санын шектемеңіз. Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	180 күн

Басқару серверінің ескерту оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Жиі болатын оқиға анықталды		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Басқару сервері басқарылатын құрылғыда жиі болатын оқиғаларды тіркейтін болса, осы түрдегі оқиғалар орын алады. Қосымша ақпаратты келесі бөлімдерден қараңыз: Жиі оқиғаларды бұғаттау.	90 күн
Лицензиялық шектеу асырылды	4098	KLSRV_EV_LICENSE_CHECK_100_110	Күніне бір рет Kaspersky Security Center бағдарламасы лицензиялық шектеудің асып кетпегенін тексеріп тұрады. Осы түрдегі оқиғалар, Басқару сервері клиент құрылғыларына орнатылған Kaspersky бағдарламаларының лицензиялық шектеуінің асып кеткенін тіркесе және бір лицензияның қолданылатын лицензиялық бірліктерінің саны лицензия қамтитын бірліктердің жалпы саны 100%-дан 110%-ға дейін құраса туындайды. Осы оқиға туындаса да, клиент құрылғылары қорғалған. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқарылатын құрылғылардың тізімін қарап шығыңыз. Қолданылмайтын құрылғыларды жойыңыз. • Көптеген құрылғыларға лицензия беріңіз (Басқару серверіне басқа жарамды белсендіру кодын немесе кілт файлын қосыңыз). Kaspersky Security Center бағдарламасы, лицензиялық шектеуден асып кеткен жағдайда оқиғаларды жасау ережесін айқындайды.	90 күн
Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Осы түрдегі оқиғалар, басқарылатын құрылғы бірнеше уақыт бойы белсенді емес болған кезде туындайды. Көбінесе, басқарылатын құрылғы істен шыққан жағдайда туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Құрылғыны басқарылатын құрылғылар тізімінен қолмен жойыңыз. • Басқару консолі көмегімен немесе Kaspersky Security Center Web Console көмегімен **Құрылғы желіде ұзақ уақыт бойы белсенді емес болып қалды** оқиғасы жасалатын уақыт аралығын көрсетіңіз. • Құрылғы Басқару консолінің немесе Kaspersky Security Center Web Console веб-консолінің көмегімен автоматты түрде жойылатын уақыт аралығын көрсетіңіз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Құрылғылар атауларының қайшылығы	4102	KLSRV_EVENT_HOSTS_CONFLICT	Осы түрдегі оқиғалар, егер Басқару сервері екі немесе одан да көп басқарылатын құрылғыны бір құрылғы ретінде қарастырған кезде туындайды. Көбінесе, клондалған қатты диск бағдарламаларды басқарылатын құрылғыларда орналастыру үшін және Желілік агентті эталонды құрылғыда бөлектелген дискіні клондау режиміне ауыстырып қоспай қолданылған кезде туындайды. Бұл мәселені болдырмау үшін, осы құрылғының қатты дискісін клондаудың алдында Желілік агентті эталонды құрылғыда дискіні клондау режиміне ауыстырып қосыңыз.	90 күн
Құрылғының күйі: "Ескерту"	4114	KLSRV_HOST_STATUS_WARNING	Осы түрдегі оқиғалар, басқарылатын құрылғыға *Ескерту* күйі тағайындалса туындайды. Сіз шарттарды конфигурациялай аласыз, оларды орындау кезінде құрылғының күйі *Ескерту* болып өзгереді.	90 күн
Лицензиялы бағдарламалар топтарының біреуі үшін орнатулар санының шектеуі жақын арада асырылады	4127	KLSRV_INVLICPROD_FILLED	Лицензиялық бағдарламалар тобына қосылған үшінші тарап бағдарламаларын орнату саны лицензиялық кілттің сипаттарында көрсетілген ең жоғары рұқсат етілген мәннің 90%-на жетсе, осы типтегі оқиғалар туындайды. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Егер үшінші тарап бағдарламасы басқарылатын құрылғыларда қолданылмаса, бағдарламаны сол құрылғылардан жойыңыз. • Жақын арада үшінші тарап бағдарламасына арналған орнату саны рұқсат етілген шектен асады деп күтсеңіз, көптеген құрылғыларға үшінші тарап бағдарламасының лицензиясын алу мүмкіндігін алдын ала қарастырыңыз. Лицензиялы бағдарламалар тобының функционалдылығын қолдана отырып, лицензиялы бағдарламалардың лицензиялық кілттерін басқара аласыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Сертификат сұралды	4133	KLSRV_CERTIFICATE_REQUESTED	Ұялы құрылғыларды басқару үшін сертификатты автоматты түрде қайта шығару мүмкін болмаса, осы түрдегі оқиғалар туындайды. Төменде оқиғалардың ықтимал себептері және оқиғаға жауап беру бойынша тиісті әрекеттер берілген: • Автоматты түрде қайта шығару, **Мүмкін болса, сертификатты автоматты түрде қайта шығару** параметрі өшірілген сертификат үшін басталды. Бұл жағдай, сертификат жасау кезінде пайда болған қатеге байланысты болуы мүмкін. Сертификатты қолмен қайта шығару қажет болуы мүмкін. • Егер сіз жалпыға ортақ инфрақұрылымымен біріктіруді қолдансаңыз, оның себебі PKI-мен біріктіру және сертификат шығару үшін қолданылатын есептік жазбаның SAM-Account-Name атрибутының болмауына байланысты болуы мүмкін. Есептік жазба сипаттарын қарап шығыңыз.	90 күн
Сертификат жойылды	4134	KLSRV_CERTIFICATE_REMOVED	Егер әкімші Ұялы құрылғыларды басқару үшін кез келген түрдегі сертификатты (жалпы, пошталық, VPN) жойса, осы түрдегі оқиғалар туындайды. Сертификат жойылғаннан кейін, осы сертификатқа қосылған ұялы құрылғылар Басқару серверіне қосыла алмайды. Бұл оқиға Ұялы құрылғыларды басқаруға қатысты ақауларды зерттеуде пайдалы болуы мүмкін.	90 күн
Сертификаттың мерзімі өтеді	6128	ServerCertificateExpiresSoon	Осы түрдегі оқиғалар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару сервері сертификаттарының жарамдылық мерзімі аяқталғанда туындайды. Сізге жарамдылық мерзімі бітейін деп жатқан сертификатты жаңарту керек.	90 күн
APNs сертификатының жарамдылық мерзімі бітті	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Осы түрдегі оқиғалар, APNs сертификатының жарамдылық мерзімі бітейін деп жатқан кезде туындайды. Сізге қолмен APNs сертификатын жаңарту және оны iOS MDM серверіне орнату қажет.	Сақталмайды

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
APNs сертификатының жарамдылық мерзімі бітейін деп жатыр	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Егер APNs сертификатының жарамдылық мерзімінің аяқталуына дейін 14 күннен аз уақыт қалса, осы түрдегі оқиғалар орын алады. APNs сертификатының жарамдылық мерзімі аяқталғаннан кейін, қолмен APNs сертификатын жаңартып, оны iOS MDM серверіне орнату керек. APNs сертификатын жарамдылық мерзімі аяқталғанға дейін жаңартуды жоспарлау ұсынылады.	Сақталмайды
FCM хабарын ұялы құрылғыға жіберу сәтсіз аяқталды	4138	KLSRV_GCM_DEVICE_ERROR	Бұл түрдегі оқиғалар Ұялы құрылғыларды басқару Android операциялық жүйесі бар басқарылатын ұялы құрылғыларға қосылу үшін Firebase Cloud Messaging (FCM) пайдалануға конфигурацияланған болса, ал FCM сервері Басқару серверінен алынған кейбір сұрауларды өңдей алмаса туындайды. Бұл дегеніміз, кейбір басқарылатын ұялы құрылғылар push хабарландыруын алмайды. Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз. FCM серверінен алынған HTTP кодтары және олармен байланысты қателер туралы қосымша ақпарат Firebase қызметінің құжаттамасында бар ("Downstream message error response codes" тарауын қараңыз).	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
FCM хабарын FCM серверіне жіберу кезінде туындаған HTTP қатесі	4139	KLSRV_GCM_HTTP_ERROR	Бұл түрдегі оқиғалар Ұялы құрылғыларды басқару Android операциялық жүйесімен басқарылатын мобильді құрылғыларды қосу үшін Firebase Cloud Messaging (FCM) пайдалануға конфигурацияланған болса және FCM сервері 200 (OK) емес HTTP коды бар Басқару серверіне салынған сұрауды қайтарса туындайды. Төменде оқиғалардың ықтимал себептері және оқиғаға жауап беру бойынша тиісті әрекеттер берілген: • FCM серверінің жағындағы мәселелер. Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз. FCM серверінен алынған HTTP кодтары және олармен байланысты қателер туралы қосымша ақпарат Firebase қызметінің құжаттамасында бар ("Downstream message error response codes" тарауын қараңыз). • Прокси-сервер жағындағы мәселелер (прокси-серверді қолдансаңыз). Оқиғаның сипаттамасындағы HTTP кодын оқып, соған сәйкес жауап беріңіз.	90 күн
FCM хабарын FCM серверіне жіберу сәтсіз аяқталды	4140	KLSRV_GCM_GENERAL_ERROR	Бұл түрдегі оқиғалар Firebase Cloud Messaging атты HTTP протоколымен жұмыс істеу кезінде Басқару сервері жағындағы күтпеген қателерден туындайды. Оқиғаның сипаттамасындағы ақпаратты оқып, оларға тиісінше ден қойыңыз. Егер сіз мәселенің шешімін өзіңіз таба алмасаңыз, Kaspersky Техникалық қолдау қызметіне хабарласуды ұсынамыз.	90 күн
Қатты дискіде бос орын аз	4105	KLSRV_NO_SPACE_ON_VOLUMES	Бұл түрдегі оқиғалар, Басқару сервері орнатылған құрылғыда диск кеңістігі таусылуға жақын қалған жағдайда туындайды. Құрылғыдағы диск кеңістігін босатыңыз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Басқару серверінің дерекқорында бос орын аз	4106	KLSRV_NO_SPACE_IN_DATABASE	Бұл түрдегі оқиғалар Басқару сервері дерекқорында бос орын шектеулі болған жағдайда орын алады. Егер сіз бұл мәселені шешпесеңіз, көп ұзамай Басқару сервері дерекқоры өзінің сыйымдылығына жетеді және Басқару сервері жұмыс істемей қалады. Төменде, қолданылатын ДҚБЖ жүйесіне тәуелді оқиғаның туындау себептері және оқиғаға ден қоюдың тиісті тәсілдері келтірілген. Сіз SQL Server Express Edition қолданасыз: • SQL Server Express құжаттамасында, қолданылатын нұсқа үшін дерекқор өлшеміне қойылған шектеуді тексеріңіз. Басқару серверіңіздің дерекқоры дерекқор өлшемінің шегіне жеткен болса керек. • Басқару серверінің дерекқорында сақталатын оқиғалар санын шектеңіз. • Басқару сервері дерекқорында бағдарламаларды басқару құрамдасы жіберген оқиғалар өте көп. Басқару серверінің дерекқорында Бағдарламаларды басқару құрамдасының оқиғаларын сақтауға қатысты Kaspersky Endpoint Security for Windows саясатының параметрлерін өзгертуге болады. SQL Server Express Edition жүйесінен ерекшеленетін ДҚБЖ қолданасаңыз: • Басқару серверінің дерекқорында сақталатын оқиғалар санын шектемеңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз. ДҚБЖ таңдау туралы ақпаратты қарап шығыңыз.	90 күн
Қосалқы Басқару серверімен байланыс үзілді	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Бұл түрдегі оқиғалар қосалқы Басқару серверімен байланыс үзілген кезде пайда болады. Қосалқы Басқару сервері орнатылған құрылғыдағы Kaspersky Event журналын оқып, соған сәйкес әрекет етіңіз.	90 күн
Негізгі Басқару серверімен байланыс үзілді	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Бұл түрдегі оқиғалар негізгі Басқару серверімен байланыс үзілген кезде пайда болады. Негізгі Басқару сервері орнатылған құрылғыдағы Kaspersky Event журналын оқып, соған сәйкес әрекет етіңіз.	90 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Kaspersky қолданбасы модульдерінің жаңа жаңартулары тіркелді	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Бұл түрдегі оқиғалар, Басқару сервері, орнатуды мақұлдауды қажет ететін басқарылатын құрылғыларда орнатылған Kaspersky бағдарламаларының жаңа жаңартуларын тіркеген жағдайда орын алады. Басқару консолі немесе Kaspersky Security Center Web Console арқылы жаңартуларды растаңыз немесе қабылдамаңыз.	90 күн
Дерекқордағы оқиғалар санының шектеуі асырылды, оқиғаларды жою басталған	4145	KLSRV_EVP_DB_TRUNCATING	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорынан ескі оқиғаларды жою, Басқару сервері дерекқорында сақталатын оқиғалардың максималды санына жеткеннен кейін басталған жағдайда орын алады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды санын көрсетіңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз.	Сақталмайды
Дерекқордағы оқиғалар санының шектеуі асырылды, оқиғалар жойылған	4146	KLSRV_EVP_DB_TRUNCATED	Мұндай түрдегі оқиғалар, Басқару сервері дерекқорында сақталатын оқиғалардың максималды санына жеткеннен кейін Басқару сервері дерекқорынан ескі оқиғаларды жойылған жағдайда орын алады. Сіз оқиғаға келесі тәсілдермен жауап бере аласыз: • Басқару серверінің дерекқорында сақталатын оқиғалардың максималды рұқсат етілген санын көрсетіңіз. • Басқару серверінің дерекқорында сақталатын оқиғалар тізімін қысқартыңыз.	Сақталмайды
Аудит (SIEM серверімен байланысты сынау сәтсіз аяқталды)	5120	KLAUD_EV_SIEM_TEST_FAILED	Бұл түрдегі оқиғалар SIEM серверіне қосылу сынағы сәтсіз аяқталған кезде туындайды.	30 күн
Сертификатты автоматты түрде беру мүмкін болмады		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Бұл оқиға мобильдік құрылғы (мобильдік протокол бойынша жұмыс істейтін құрылғы) үшін клиент сертификатын жасау қатесі болған жағдайда орын алады.	90 күн

Басқару серверінің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center Басқару серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға және конфигурациялауға болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Басқару серверінің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі	Пікір
Лицензиялық кілттің 90%-дан көп бөлігі қолданылып қойған	4097	KLSRV_EV_LICENSE_CHECK_90	30 күн	
Жаңа құрылғы анықталды	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 күн	
Құрылғы топқа автоматты түрде қосылды	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 күн	
Құрылғы ереже арқылы автоматты түрде жылжытылды	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 күн	
Құрылғы топтан жойылды: желіде ұзақ уақыт бойы белсенді емес	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 күн	
Лицензиялы бағдарламалар топтарының біреуі үшін рұқсат етілген орнатулардың саны (95%-дан) асты	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 күн	
Kaspersky талдауға жіберетін файлдар пайда болды	4131	KLSRV_APS_FILE_APPEARED	30 күн	
Осы ұялы құрылғыда FCM үлгісінің идентификаторы өзгертілді	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 күн	
Жаңартулар белгіленген қалтаға сәтті көшірілді	4122	KLSRV_UPD_REPL_OK	30 күн	
Қосалқы Басқару серверімен байланыс орнатылды	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 күн	
Негізгі Басқару серверімен байланыс орнатылды	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 күн	
Дерекқорлар жаңартылды	4144	KLSRV_UPD_BASES_UPDATED	30 күн	
Аудит: Басқару серверіне қосылым орнатылды	4147	KLAUD_EV_SERVERCONNECT	30 күн	Бұл түрдегі оқиғалар пайдаланушы басқару серверіне басқару консолі немесе Kaspersky Security Center Web Console арқылы қосылғанда орын алады. Бұл оқиғалар MMC негізіндегі басқару консолі немесе Kaspersky Security Center Web Console Server орнатылған құрылғының IP мекенжайы туралы ақпаратты қамтиды.

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі	Пікір
Аудит: нысан өзгертілді	4148	KLAUD_EV_OBJECTMODIFY	30 күн	Бұл оқиға келесі нысандардағы өзгерістерді қадағалайды: • Басқару тобы • Қауіпсіздік тобы • Пайдаланушы • Орнату пакеттері • Тапсырма • Саясат • Сервер • Виртуалды сервер
Аудит: нысан күйі өзгертілді	4150	KLAUD_EV_TASK_STATE_CHANGED	30 күн	Мысалы, тапсырма қатемен аяқталса, бұл оқиға туындайды.
Аудит: топ параметрлері өзгертілді	4149	KLAUD_EV_ADMGROUP_CHANGED	30 күн	
Аудит: Басқару серверіне қосылу тоқтатылды	4151	KLAUD_EV_SERVERDISCONNECT	30 күн	
Аудит: Нысанның сипаттары өзгертілді	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 күн	Бұл оқиға келесі параметрлердегі өзгерістерді қадағалайды: • Пайдаланушы • Лицензия • Сервер • Виртуалды сервер
Аудит: Пайдаланушы рұқсаттары өзгертілді	4153	KLAUD_EV_OBJECTACLMODIFIED	30 күн	
Аудит: Басқару серверінен импортталған немесе экспортталған шифрлау кілттері	5100	KLAUD_EV_DPEKEYSEXPORT	30 күн	
Аудит: SIEM серверімен сынақ байланысын орнату сәтті аяқталды	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 күн	Бұл оқиға SIEM серверінің қосылымы сәтті орнатылған кезде пайда болады.
Резервтік сертификат жасалды		ServerReserveCertificateCreated	30 күн	Бұл оқиға басқару серверінің сертификаты жасалған кезде пайда болады.
Сертификат мерзімін ұзарту		ServerCertificateRenewed	30 күн	Бұл оқиға басқару серверінің сертификаты жаңартылған кезде орын алады.

Резервтік сертификат жасалды және **Сертификат мерзімін ұзарту** оқиғаларына сәйкес келетін операциялар мобильдік құрылғылар мен UEFI құрылғыларына арналған басқару серверінің сертификаттары үшін орындалғанда ғана, осы оқиғалар басқару сервері арқылы автоматты түрде жарияланады және басқару консолінде көрсетіледі.

Желілік агент оқиғалары

Бұл бөлімде Желілік агент оқиғалары туралы ақпарат бар.

Желілік агенттің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center Желілік агентінің оқиға түрлері келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Жаңартуды орнату қатесі	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Осындай түрдегі оқиғалар, Kaspersky Security Center құрамдастары үшін жаңартулар мен патчтарды автоматты түрде орнату сәтсіз аяқталған кезде туындайды. Оқиға, Kaspersky басқарылатын бағдарламаларының жаңартуларына жатпайды. Оқиғаның сипаттамасын оқыңыз. Бұл оқиғаның себебі, Басқару серверіндегі Windows операциялық жүйесінің мәселесі болуы мүмкін. Егер сипаттамада Windows конфигурациясының қандай да бір мәселесі туралы айтылса, бұл мәселені шешіңіз.	30 күн
Үшінші тарап бағдарламалық жасақтамасы жаңартуын орнату сәтсіз болды	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Осындай түрдегі оқиғалар, Осалдықтар мен патчтарды басқару және Ұялы құрылғыларды басқару мүмкіндіктері қолданылып жатса және үшінші тарап өндірушілерінің бағдарламалық жасақтамасын жаңарту сәтсіз аяқталған болса туындайды. Үшінші тарап бағдарламасына келтірілген сілтеменің дұрыс екенін тексеріңіз. Оқиғаның сипаттамасын оқыңыз.	30 күн
Windows Update жаңартуларын орнату сәтсіз аяқталды	7717	KLNAG_EV_WUA_INSTALL_ERROR	Осындай түрдегі оқиғалар, егер Windows Update жаңартулары сәтсіз аяқталған болса туындайды. Microsoft Windows жаңартуларын Желілік агент саясатында конфигурациялаңыз. Оқиғаның сипаттамасын оқыңыз. Microsoft білім қорындағы қатенің сипаттамасын іздеп көріңіз. Егер сіз мәселені өзіңіз шеше алмасаңыз, Microsoft техникалық қолдау қызметіне хабарласыңыз.	30 күн
Пайдаланушыларды басқару: қателер	7723	KLNAG_EV_USR_MNG_ERR	Жалпы ескерту оқиғасы.	30 күн
Sudoers файлын сілтемелік мәнге қалпына келтіру сәтсіз аяқталды	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Оқиға sudoers файлын ауыстыру қатесінің сипаттамасын қамтиды.	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Сипаттамасы	Әдепкі бойынша сақтау мерзімі
Түбірлік сертификаттарды орнату сәтсіз аяқталды	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Оқиға сертификаттарды орнату қатесінің сипаттамасын қамтиды.	30 күн
Түбірлік сертификаттарды өшіру сәтсіз аяқталды	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Оқиға сертификаттарды жою қатесінің сипаттамасын қамтиды.	30 күн

Желілік агенттің ескертулері оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center Желілік агентінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің ескертулері оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бағдарламалық модуль жаңартуын орнату кезінде ескерту пайда болды	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату ескертумен аяқталды	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату кейінге қалдырылды	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 күн
Қауіпсіздік мәселесі пайда болды	549	GNRL_EV_APP_INCIDENT_OCCURED	30 күн
KSN Проксиі іске қосылды. KSN қолжетімділігін тексеру сәтсіз аяқталды	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 күн
Пайдаланушыларды басқару: ескертулер	7722	KLNAG_EV_USR_MNG_WRN	30 күн
Табылған sudoers файлы сілтемелік мәнге сәйкес келмейді	7724	KLNAG_EV_SUDOER_DIFFERENT	30 күн

Желілік агенттің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center Желілік агентінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

Желілік агенттің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бағдарламалық модульдерінің жаңартуы сәтті орнатылды	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 күн
Бағдарламалық модуль жаңартуын орнату басталды	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 күн
Бағдарлама орнатылды	7703	KLNAG_EV_INV_APP_INSTALLED	30 күн
Бағдарлама жойылды	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 күн
Бақыланатын бағдарлама орнатылды	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі идентификаторы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бақыланатын бағдарлама жойылды	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 күн
Үшінші тарап бағдарламасы орнатылды	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 күн
Жаңа құрылғы қосылды	7708	KLNAG_EV_DEVICE_ARRIVAL	30 күн
Құрылғы жойылды	7709	KLNAG_EV_DEVICE_REMOVE	30 күн
Жаңа құрылғы анықталды	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 күн
Құрылғы авторизацияланды	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: файл оқылды	7712	KLUSRLOG_EV_FILE_READ	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: файл өзгертілді	7713	KLUSRLOG_EV_FILE_MODIFIED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: бағдарлама іске қосылды	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: басталды	7715	KLUSRLOG_EV_WDS_BEGIN	30 күн
Windows компьютерлік бөлісу қызметін пайдалану: тоқтатылды	7716	KLUSRLOG_EV_WDS_END	30 күн
Үшінші тарап бағдарламалық жасақтамасының жаңартуы сәтті орнатылды	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 күн
Үшінші тарап бағдарламалық жасақтаманың жаңартуын орнату басталды	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 күн
KSN Проксиі іске қосылды. KSN қолжетімділігін тексеру сәтті аяқталды	7719	KSNPROXY_STARTED_CON_CHK_OK	30 күн
KSN Проксиі тоқтатылды	7720	KSNPROXY_STOPPED	30 күн

iOS MDM сервері оқиғалары

Бұл бөлімде iOS MDM сервері оқиғалары туралы ақпарат бар.

iOS MDM серверінің функционалдық ақауы оқиғалары

Төмендегі кестеде **Функционалдық ақау** маңыздылық деңгейі бар Kaspersky Security Center iOS MDM серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

iOS MDM серверінің функционалдық ақауы оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Профильдер тізімін сұрау мүмкін болмады	PROFILELIST_COMMAND_FAILED	30 күн
Профильді орнату мүмкін болмады	INSTALLPROFILE_COMMAND_FAILED	30 күн
Профильді жою мүмкін болмады	REMOVEPROFILE_COMMAND_FAILED	30 күн
Provisioning профильдерінің тізімін сұрау мүмкін болмады	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 күн
Provisioning профилін орнату мүмкін болмады	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 күн

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Provisioning профилін жою мүмкін болмады	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 күн
Цифрлық сертификаттардың тізімін сұрау мүмкін болмады	CERTIFICATELIST_COMMAND_FAILED	30 күн
Орнатылған бағдарламалар тізімін сұрау мүмкін болмады	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 күн
Ұялы құрылғы туралы жалпы ақпаратты сұрау мүмкін болмады	DEVICEINFORMATION_COMMAND_FAILED	30 күн
Қауіпсіздік туралы ақпаратты сұрау мүмкін болмады	SECURITYINFO_COMMAND_FAILED	30 күн
Ұялы құрылғыны бұғаттау мүмкін болмады	DEVICELOCK_COMMAND_FAILED	30 күн
Құпиясөзді тазалау мүмкін болмады	CLEARPASSCODE_COMMAND_FAILED	30 күн
Ұялы құрылғының деректерін жою мүмкін болмады	ERASEDEVICE_COMMAND_FAILED	30 күн
Қосымшаны орнату мүмкін болмады	INSTALLAPPLICATION_COMMAND_FAILED	30 күн
Қосымша үшін өтеу кодын орнату мүмкін болмады	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 күн
Басқарылатын бағдарламалар тізімін сұрау мүмкін болмады	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 күн
Басқарылатын қосымшаны жою мүмкін болмады	REMOVEAPPLICATION_COMMAND_FAILED	30 күн
Роуминг параметрлері қабылданбады	SETROAMINGSETTINGS_COMMAND_FAILED	30 күн
Қолданба жұмысында қате пайда болды	PRODUCT_FAILURE	30 күн
Пәрменді орындау нәтижесі дұрыс емес деректерді қамтиды	MALFORMED_COMMAND	30 күн
Push-хабарландыруды жіберу сәтсіз болды (Push Notification)	SEND_PUSH_NOTIFICATION_FAILED	30 күн
Пәрменді жіберу мүмкін болмады	SEND_COMMAND_FAILED	30 күн
Құрылғы табылмады	DEVICE_NOT_FOUND	30 күн

iOS MDM серверінің ескерту оқиғалары

Төмендегі кестеде **Ескерту** маңыздылық деңгейі бар Kaspersky Security Center iOS MDM серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

iOS MDM серверінің ескерту оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Бұғатталған ұялы құрылғыны қосу әрекеті	INACTICE_DEVICE_TRY_CONNECTED	30 күн
Профильді жою	MDM_PROFILE_WAS_REMOVED	30 күн
Клиенттік сертификатты қайтадан пайдалану әрекеті	CLIENT_CERT_ALREADY_IN_USE	30 күн
Белсенді емес құрылғы анықталды	FOUND_INACTIVE_DEVICE	30 күн
Өтеу коды керек	NEED_REDEMPTION_CODE	30 күн
Профиль құрылғыдан жойылған саясатқа қосылды	UMDM_PROFILE_WAS_REMOVED	30 күн

iOS MDM серверінің ақпараттық оқиғалары

Төмендегі кестеде **Ақпараттық** маңыздылық деңгейі бар Kaspersky Security Center iOS MDM серверінің оқиғалары келтірілген.

Бағдарлама жасай алатын әрбір оқиға үшін, бағдарлама саясаты сипаттарындағы **Оқиғаларды конфигурациялау** қойындысында хабарландыру параметрлерін және сақтау параметрлерін көрсетуге болады. Барлық оқиғалар үшін хабарландыру параметрлерін бірден конфигурациялау қажет болса, Басқару сервері сипаттарында жалпы хабарландыру параметрлерін конфигурациялаңыз.

iOS MDM серверінің ақпараттық оқиғалары

Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Әдепкі бойынша сақтау мерзімі
Жаңа ұялы құрылғы қосылды	NEW_DEVICE_CONNECTED	30 күн
Профильдер тізімін сұрау сәтті орындалды	PROFILELIST_COMMAND_SUCCESSFULL	30 күн
Профильді орнату сәтті орындалды	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 күн
Профильді жою сәтті орындалды	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 күн
Provisioning профильдерінің тізімін сұрау сәтті орындалды	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 күн
Provisioning профилін орнату сәтті орындалды	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 күн
Provisioning профилін жою сәтті орындалды	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 күн
Цифрлық сертификаттардың тізімін сұрау сәтті орындалды	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 күн
Орнатылған бағдарламалар тізімін сұрау сәтті орындалды	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 күн
Ұялы құрылғы туралы жалпы ақпаратты сұрау сәтті орындалды	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 күн
Қауіпсіздік туралы ақпаратты сұрау сәтті орындалды	SECURITYINFO_COMMAND_SUCCESSFULL	30 күн
Ұялы құрылғы сәтті бұғатталды	DEVICELOCK_COMMAND_SUCCESSFULL	30 күн
Құпиясөзді тазалау сәтті орындалды	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 күн
Деректер ұялы құрылғыдан жойылды	ERASEDEVICE_COMMAND_SUCCESSFULL	30 күн
Қосымшаны орнату сәтті орындалды	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 күн
Қосымша үшін өтеу кодын орнату сәтті өтті	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 күн
Басқарылатын бағдарламалар тізімін сұрау сәтті орындалды	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 күн
Басқарылатын қолданба сәтті жойылды	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 күн
Роуминг параметрлері сәтті қолданылды	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 күн

Жиі болатын оқиғаларды бұғаттау

Бұл бөлімде жиі болатын оқиғаларды бұғаттауды басқару және жиі болатын оқиғаларды бұғаттауды болдырмау туралы ақпарат берілген.

Жиі болатын оқиғаларды бұғаттау туралы

Бір немесе бірнеше басқарылатын құрылғыларда орнатылған Kaspersky Endpoint Security for Windows сияқты басқарылатын бағдарлама Басқару серверіне көптеген бір тіпті оқиғаларды жібере алады. Жиі болатын оқиғаларды қабылдау Басқару сервері дерекқорының шамадан тыс жүктелуіне және басқа оқиғалардың қайта жазылуына әкелуі мүмкін. Басқару сервері барлық алынған оқиғалар саны дерекқор үшін белгіленген шектен асқан кезде ең жиі болатын оқиғаларды бұғаттай бастайды.

Басқару сервері жиі болатын оқиғаларды автоматты түрде бұғаттайды. Сіз жиі болатын оқиғаларды өзіңіз бұғаттай алмайсыз немесе қандай оқиғаларды бұғаттауды таңдай алмайсыз.

Оқиғаның бұғатталғанын білу үшін, хабарландырулар тізімін көруге немесе бұл оқиғаның **Жиі болатын оқиғаларды бұғаттау** бөліміндегі Басқару сервері сипаттарында бар-жоғын көруге болады. Егер оқиға бұғатталған болса, келесі әрекеттерді орындауға болады:

- Дерекқордың қайта жазылуына жол бергіңіз келмесе, оқиғалардың осы түрін алуға тыйым салуды жалғастыра аласыз.
- Егер сіз, мысалы, жиі болатын оқиғаларды Басқару серверіне жіберудің себебін білгіңіз келсе, сіз жиі болатын оқиғалардың құлпын ашып, кез келген жағдайда оқиғалардың осы түрін алуды жалғастыра аласыз.
- Егер сіз жиі болатын оқиғаларды қайтадан бұғатталғанға дейін жалғастырғыңыз келсе, жиі болатын оқиғаларды бұғаттауды болдырмауға болады.

Жиі болатын оқиғаларды бұғаттауды басқару

Басқару сервері жиі болатын оқиғаларды алуды автоматты түрде бұғаттайды, бірақ сіз жиі болатын оқиғалардың құлпын ашып, оларды алуды жалғастыра аласыз. Сондай-ақ, бұрын құлпы ашылған жиі болатын оқиғаларды алуға тыйым салуға болады.

Жиі болатын оқиғады бұғаттуды басқару үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жиі болатын оқиғаларды бұғаттау** бөлімін таңдаңыз.

3. **Жиі болатын оқиғаларды бұғаттау** бөлімінде:

   - Егер сіз жиі болатын оқиғалардың құлпын ашқыңыз келсе:

     a. Құлпын ашқыңыз келетін жиі болатын оқиғаларды таңдап, **Есептен шығару** түймесін басыңыз.

     b. **Сақтау** түймесін басыңыз.

   - Жиі болатын оқиғаларды қабылдауды бұғаттағыңыз келсе:

     a. Бұғаттағыңыз келетін жиі болатын оқиғаларды таңдап, **Бұғаттау** түймесін басыңыз.

     b. **Сақтау** түймесін басыңыз.

Басқару сервері құлпы ашылған жиі болатын оқиғаларды қабылдайды және бұғатталған жиі болатын оқиғаларды қабылдамайды.

Жиі болатын оқиғады бұғаттауды болдырмау

Сіз жиі болатын оқиғаларды бұғаттаудан бас тарта аласыз және Басқару сервері осы жиі болатын оқиғаларды қайтадан бұғаттағанға дейін, оқиғаларды алуды бастай аласыз.

Жиі болатын оқиғаларды бұғаттауды болдырмау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Жиі болатын оқиғаларды бұғаттау** бөлімін таңдаңыз.

3. **Жиі болатын оқиғаларды бұғаттау** бөлімінде бұғаттуды болдырмағыңыз келетін жиі болатын оқиға жолын басыңыз.

4. **Бұғаттаудан жою** түймесін басыңыз.

Жиі болатын оқиға жиі болатын оқиғалар тізімінен жойылады. Басқару сервері осы түрдегі оқиғаларды алып тұрады.

Хабарландырулар және құрылғылар күйлері

Бұл бөлімде хабарландыруларды көру, хабарландыруларды жеткізуді конфигурациялау, құрылғылардың күйін пайдалану және құрылғы күйлерін өзгертуді қосу тәсілі туралы ақпарат бар.

Хабарландыруларды қолдану

Хабарландырулар оқиғалар туралы ескертуге және сіз сәйкес деп санайтын ұсынылған әрекеттерді орындау арқылы осы оқиғаларға жауап беру жылдамдығыңызды арттыруға көмектесу үшін жасалған.

Таңдалған хабарландыру тәсіліне байланысты келесі хабарландыру түрлері қолжетімді:

- Экрандағы хабарландырулар
- SMS хабарландыруы
- Электрондық пошта арқылы хабарлау
- Орындалатын файлды немесе сценарийді іске қосу арқылы хабарландыру

Экрандағы хабарландырулар

Экрандағы хабарландырулар маңыздылық деңгейлері бойынша топтастырылған оқиғалар туралы ескертеді (*Критикалық хабарландыру*, *Ескерту хабарландыруы*, және *Ақпараттық хабарландыру*).

Экрандағы хабарландырулар екі күйдің біріне ие болуы мүмкін:

- *Қаралды*. Бұл, хабарландыру үшін ұсынылған әрекетті орындағаныңызды немесе осы күйді қолмен хабарлау үшін тағайындағаныңызды білдіреді.
- *Қаралған жоқ*. Бұл, хабарландыру үшін ұсынылған әрекетті орындамағаныңызды немесе осы күйді қолмен хабарлау үшін тағайындамағаныңызды білдіреді.

Әдепкі бойынша, хабарландырулар тізіміне *Қаралған жоқ* мәртебесі бар хабарландырулар кіреді.

Өз ұйымыңыздың желісін экрандағы хабарландыруларды көру және оларға нақты уақыт режимінде жауап беру арқылы басқара аласыз.

Электрондық пошта, SMS бойынша және орындалатын файлды немесе скриптті іске қосу арқылы хабарландыру

Kaspersky Security Center бағдарламасы маңызды деп санайтын оқиғалар туралы хабарландырулар жіберу арқылы ұйымыңыздың желісін басқаруға мүмкіндік береді. Кез келген оқиға үшін электрондық пошта, SMS бойынша немесе орындалатын файлды немесе скриптті іске қосу арқылы хабарландыруларды конфигурациялауға болады.

SMS немесе электрондық пошта бойынша хабарландыру алғаннан кейін, сіз оқиғаға жауап беру туралы шешім қабылдай аласыз. Бұл жауап сіздің ұйымыңыздың желісі үшін ең қолайлы болуы керек. Орындалатын файлды немесе скриптті іске қосу арқылы сіз оқиғаның жауабын алдын ала анықтайсыз. Сондай-ақ, оқиғаға негізгі жауап ретінде орындалатын файлды немесе скриптті іске қосуды қарастыруға болады. Орындалатын файлды іске қосқаннан кейін, оқиғаға жауап беру үшін басқа қадамдар жасауға болады.

Экрандағы хабарландыруларды қарау

Экрандағы хабарландыруларды үш тәсілмен көруге болады:

- **Бақылау және есеп беру** → **Хабарландырулар** бөлімінде. Мұнда алдын ала анықталған санаттарға қатысты хабарландыруларды көруге болады.
- Қазіргі уақытта қандай бөлімді пайдалансаңыз да ашуға болатын бөлек терезеде. Бұл жағдайда, сіз хабарландыруларды қаралған деп белгілей аласыз.
- **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміндегі **Таңдалған қауіптілік деңгейі бойынша хабарландырулар** веб-виджетінде. Бұл веб-виджетте сіз тек *Критикалық* және *Ескерту* маңыздылық деңгейі бар хабарландыруларды ғана қарай аласыз.

Сіз оқиғаға жауап беру сияқты әрекеттерді орындай аласыз.

Алдын ала анықталған санат хабарландыруларын көру үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Хабарландырулар** бөліміне өтіңіз.

   Сол жақ тақтада **Барлық хабарландырулар** санаты таңдалған, ал сол жақта барлық хабарландырулар көрсетіледі.

2. Сол жақ тақтадан келесі санаттардың бірін таңдаңыз:

   - **Орналастыру**
   - **Құрылғылар**
   - **Қорғаныс**
   - **Жаңартулар** (бұған жүктеуге болатын Kaspersky бағдарламалары туралы хабарландырулар және жүктелген антивирустық дерекқор жаңартулары туралы хабарландырулар кіреді)
   - **Эксплойттан қорғаныс**
   - **Басқару сервері** (бұл хабарландыру тек Басқару серверіне қатысты оқиғаларды қамтиды)
   - **Пайдалы сілтемелер** (бұған Kaspersky ресурстарына сілтемелер, мысалы, Kaspersky Техникалық қолдау қызметіне, Kaspersky форумына, лицензияны ұзарту бетіне немесе Вирустық энциклопедияға сілтеме кіреді)

   Хабарландырулар тізімінде таңдалған санат көрсетіледі. Тізімде мыналар бар:

- Хабарландыру тақырыбына қатысты белгіше: орналастыру (), қорғаныс (), жаңартулар (), құрылғыларды басқару (), Эксплойттан қорғаныс (), Басқару сервері ().
- Хабарландырудың маңыздылық деңгейі. Келесі маңыздылық деңгейлері бар хабарландырулар көрсетіледі: **Критикалық хабарландырулар** (), **Ескерту хабарландырулары** (), **Ақпараттық хабарландырулар**. Тізімдегі хабарландырулар маңыздылық деңгейі бойынша топтастырылған.
- **Хабарландыру**. Мұнда хабарландыру сипаттамасы бар.
- **Әрекет**. Мұнда орындауға ұсынылатын жылдам әрекетке сілтеме бар. Мысалы, осы сілтеме арқылы қоймаға өтіп, қауіпсіздік бағдарламасын құрылғыларға орната аласыз, құрылғылар тізімін немесе оқиғалар тізімін қарай аласыз. Хабарландыру үшін ұсынылатын әрекетті орындағаннан кейін, бұл хабарландыруға *Қаралды* күйі беріледі.
- **Күй тіркелді**. Мұнда Басқару серверінде хабарландыру тіркелген күннен бастап өткен күндер немесе сағаттар саны бар.

Маңыздылық деңгейі бойынша бөлек терезеде экран хабарландыруларын көру үшін:

1. Kaspersky Security Center Web Console жоғарғы оң жақ бұрышында жалауша () белгішесін басыңыз.

   > Жалауша белгішесінің жанында қызыл нүкте болса, демек, қаралмаған хабарландырулар бар.

   Хабарландырулар тізімі бар терезе ашылады. Әдепкі бойынша **Барлық хабарландырулар** қойыншасы таңдалған және маңыздылық деңгейлері бойынша топтастырылған хабарландырулар көрсетіледі: *Критикалық хабарландырулар*, *Ескерту хабарландырулары* және *Ақпараттық хабарландырулар*.

2. **Жүйе** қойыншасын таңдаңыз.

   Критикалық хабарландырулар (!) және *Ескерту хабарландырулары* (⚠) маңыздылық деңгейлері бар хабарландырулар тізімі көрсетіледі. Хабарландырулар тізіміне мыналар кіреді:

   - Түсті индикатор. Критикалық хабарландырулар қызыл түспен белгіленген. Ескерту хабарландырулары сары түспен белгіленген.
   - Хабарландыру тақырыбына қатысты белгіше: орналастыру, қорғаныс, жаңартулар, құрылғыларды басқару, Эксплойттан қорғаныс, Басқару сервері.
   - Хабарландыру сипаттамасы.
   - Жалауша белгішесі. Сұр жалауша *Қаралған жоқ* күйі берілген хабарландырулар үшін пайдаланылады. Сұр жалаушаны таңдап, хабарландыру үшін *Қаралды* күйін тағайындаған кезде жалаушаның түсі ақ түске өзгереді.
   - Ұсынылатын әрекетке сілтеме. Сілтемені басу арқылы ұсынылған әрекетті орындаған кезде хабарландыруға *Қаралды* күйі беріледі.
   - Басқару серверінде хабарландыру тіркелген күннен бастап өткен күндер саны.

3. **Көбірек** қойыншасын таңдаңыз.

   Ақпараттық хабарландырулар маңыздылық деңгейі бар хабарландырулар тізімі көрсетіледі.

   Тізімнің құрылымы **Жүйе** қойыншасындағы тізім үшін сияқты (сипаттамасы жоғарыда келтірілген). Ол тек түсті индикатордың болмауымен ерекшеленеді.

Хабарландыруларды Басқару серверінде тіркелген күндер бойынша сүзгілеуге болады. Сүзгіні конфигурациялау үшін **Сүзгіні көрсету** жалаушасын қолданыңыз.

Веб-виджетте экран хабарландыруларын көру үшін:

1. **Бақылау тақтасы** бөлімінде **Веб-виджетті қосу не қалпына келтіру** тармағын таңдаңыз.
2. Ашылған терезеде **Басқа** санатын басыңыз, **Таңдалған қауіптілік деңгейі бойынша хабарландырулар** веб-виджетін таңдаңыз және Қосу түймесін басыңыз.

   Веб-виджет **Бақылау тақтасы** қойыншасында көрсетіледі. Әдепкі бойынша, веб-виджетте *Критикалық* маңыздылық деңгейі бар хабарландырулар көрсетіледі.

   Ескерту хабарландырулары маңыздылық деңгейі бар хабарландыруларды көру үшін веб-виджетте **Параметрлер** түймесін басып, веб-виджет параметрлерін өзгерте аласыз. Не болмаса, басқа веб-виджетті қоса аласыз: *Ескерту хабарландырулары* маңыздылық деңгейі бар **Таңдалған қауіптілік деңгейі бойынша хабарландырулар**.

   Веб-виджеттегі хабарландырулар тізімінің көлемі шектеулі және тек екі хабарландыруды қамтиды. Бұл екі хабарландыру соңғы оқиғаларға қатысты.

Веб-виджет хабарландыруларының тізіміне мыналар кіреді:

- Хабарландыру тақырыбына қатысты белгіше: орналастыру, қорғаныс, жаңартулар, құрылғыларды басқару, Эксплойттан қорғаныс, Басқару сервері.
- Ұсынылған әрекетке сілтеме жасалған хабарландырудың сипаттамасы. Сілтемені басу арқылы ұсынылған әрекетті орындаған кезде хабарландыруға *Қаралды* күйі беріледі.

- Басқару серверінде хабарландыру тіркелген күннен бастап өткен күндер немесе сағаттар саны.
- Басқа хабарландыруларға сілтеме. **Бақылау және есеп беру** бөлімінде **Хабарландырулар** бөліміндегі хабарландыруларды көруге арналған сілтемеден өтіңіз.

Құрылғы күйлері туралы

Kaspersky Security Center бағдарламасы әрбір басқарылатын құрылғыға күй тағайындайды. Нақты күйі, пайдаланушы анықтаған шарттардың орындалғанына байланысты. Кейбір жағдайларда Kaspersky Security Center құрылғысына күй тағайындау кезінде құрылғының желіде көрінуін ескереді (төмендегі кестені қараңыз). Мысалы, басқарылатын құрылғыға *Критикалық* күйі берілген болса, *Дерекқорлар ескірген* шарты орындалғандықтан, құрылғы үшін көзге көрінетін болғандықтан, құрылғыға *ОК* күйі беріледі. Егер Kaspersky Security Center құрылғыны екі сағат ішінде желіден таппаса, құрылғының көрінуі *Офлайн* мәніне ие болады.

Келесі күйлер бар:

- *Критикалық* немесе *Критикалық / Көзге көрінетін*.
- *Ескерту* немесе *Ескерту / Көзге көрінетін*.
- *ОК* немесе *ОК / Көзге көрінетін*.

Төмендегі кестеде құрылғыға *Критикалық* немесе *Ескерту* күйін және олардың мүмкін мәндерін тағайындау үшін әдепкі бойынша шарттар келтірілген.

Құрылғыға күйлер белгілеу шарттары

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қауіпсіздік бағдарламасы орнатылмаған	Желілік агент құрылғыға орнатылған, бірақ қауіпсіздік бағдарламасы орнатылмаған.	• Қосқыш қосулы. • Қосқыш өшірулі.
Тым көп вирус анықталды	Вирустарды іздеу тапсырмаларының, мысалы, *Зиянды БҚ іздеу* тапсырмаларының жұмысы нәтижесінде, құрылғыда вирустар табылды және анықталған вирустардың саны көрсетілген мәннен асып түседі.	0-ден артық.
Нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше	Құрылғы желіде көрінеді, бірақ құрылғы күйіне арналған шартта нақты уақыт режимінде қорғау деңгейі әкімші орнатқан деңгейден өзгеше.	• Тоқтатылды. • Кідіртілді. • Орындалуда.
Зиянды бағдарлама сканерлеуі ұзақ уақыт орындалмады	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ *Зиянды БҚ іздеу* тапсырмасы да, жергілікті тексеру тапсырмасы да көрсетілген уақыттан артық орындалмады. Шарт тек жеті күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Дерекқорлар ескірген	Құрылғы желіде көрінеді және құрылғыда қауіпсіздік бағдарламасы орнатылған, бірақ антивирустық дерекқорлар бұл құрылғыда көрсетілген уақыттан артық жаңартылмаған. Шарт тек бір күн бұрын немесе одан бұрын Басқару сервері дерекқорына қосылған құрылғыларға қолданылады.	1-күннен артық.
Қосылмағанына көп болды	Желілік агент құрылғыға орнатылған, бірақ құрылғы Басқару серверіне көрсетілген уақыттан артық қосылмаған, себебі құрылғы өшірулі.	1-күннен артық.
Белсенді қауіптер анықталды	**Белсенді қауіптер** қалтасындағы өңделмеген нысандар саны көрсетілген мәннен асып түседі.	0 данадан артық.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қайта іске қосу керек	Құрылғы желіде көрінеді, бірақ бағдарлама таңдалған себептердің біріне байланысты құрылғыны белгіленген уақыттан ұзағырақ қайта жүктеуді талап етеді.	0 минуттан көбірек.
Үйлесімді емес бағдарламалар орнатылды	Құрылғы желіде көрінеді, бірақ Желілік агент орындаған бағдарламалық жасақтаманы түгендеу кезінде, құрылғыда үйлесімсіз бағдарламалардың орнатылғаны анықталды.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарламалық жасақтама осалдықтары анықталды	Құрылғы желіде көрінеді және оған Желілік агент орнатылған, бірақ *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасын орындау нәтижесінде құрылғыда критикалық деңгейі белгіленген бағдарламаларда осалдықтар анықталды.	• Критикалық. • Жоғары. • Орташа. • Осалдықты жабу мүмкін емес болса, елемеу. • Жаңарту орнатуға белгіленген болса, елемеу.
Лицензия мерзімі өтті	Құрылғы желіде көрінеді, бірақ лицензияның жарамдылық мерзімі өтіп кеткен.	• Қосқыш өшірулі. • Қосқыш қосулы.
Лицензияның қолданылу мерзімі жақында аяқталады	Құрылғы желіде көрінеді, бірақ лицензиялық жарамдылық мерзімі көрсетілген күндер санынан аз уақыттан кейін өтіп кетеді.	0 күннен аз.
Windows Update жаңартуларын іздеу ұзақ уақыт бойы орындалмады	Құрылғы желіде көрінеді, бірақ *Windows Update жаңартуларын синхрондау* тапсырмасы көрсетілген уақыт аралығында орындалмаған.	1-күннен артық.
Жарамсыз шифрлау күйі	Желілік агент құрылғыға орнатылған, бірақ құрылғыны шифрлау нәтижесі көрсетілген мәнге тең.	• Пайдаланушының бас тартуына байланысты саясатқа сәйкес келмейді (тек сыртқы құрылғылар үшін). • Қатеге байланысты саясатқа сай емес. • Саясат қолданылуда – қайта іске қосу қажет. • Шифрлау саясаты белгіленбеген. • Қолдау көрсетілмейді. • Саясат қолданылуда.
Ұялы құрылғы параметрлері саясатқа жауап бермейді	Ұялы құрылғының параметрлері сәйкестік ережелерін тексеру кезінде Kaspersky Endpoint Security for Android саясатында белгіленген параметрлерден ерекшеленеді.	• Қосқыш өшірулі. • Қосқыш қосулы.
Өңделмеген қауіпсіздік мәселелері табылды	Құрылғыда өңделмеген қауіпсіздік мәселелері бар. Қауіпсіздік мәселелері клиенттік құрылғыға орнатылған басқарылатын Kaspersky қолданбалары арқылы автоматты түрде жасалуы немесе әкімші қолмен жасауы мүмкін.	• Қосқыш өшірулі. • Қосқыш қосулы.
Бағдарлама анықтаған құрылғы күйі	Құрылғының күйін басқарылатын бағдарлама анықтайды. Басқарылатын құрылғылар Kaspersky Security Center параметрлеріне қарамастан басқарылатын қолданбалармен анықталған күйге ие болуы мүмкін. Бұл күй Kaspersky Security Center анықтаған күйлердің бірін қайтарғаннан кейін, Басқару сервер басқарылатын құрылғыға басқарылатын құрылғы қайтарған және Басқару сервер тағайындағандардың ең маңызды күйін тағайындайды. Басқарылатын қолданбалар анықтаған күйлердің басқарылатын қолданбалар арқылы берілген сипаттамалары бар. Сипаттамаларды басқарылатын құрылғылар тізімінде, **Күйдің сипаттамасы** бағанында көре аласыз.	• Қосқыш өшірулі. • Қосқыш қосулы.
Құрылғыда бос орын жоқ	Құрылғының бос диск кеңістігі көрсетілген мәннен аз немесе құрылғы Басқару серверімен синхрондала алмайды. Құрылғы Басқару серверімен сәтті синхрондалғанда және құрылғының бос диск кеңістігі көрсетілген мәннен көп немесе тең болса, *Критикалық* немесе *Ескерту* күйлері *ОК* күйіне өзгереді.	0 МБ-тан көбірек.
Құрылғы басқарылмайтын күйге айналды	Құрылғылар табылған кезде құрылғы желіде көрінетін болып анықталады, бірақ Басқару серверімен синхрондаудың үштен артық сәтсіз әрекеті орындалды.	• Қосқыш өшірулі. • Қосқыш қосулы.

Шарт	Шарттың сипаттамасы	Қолжетімді мәндері
Қорғаныс өшірілген	Құрылғы көзге көрінеді, бірақ құрылғыдағы қауіпсіздік бағдарламасы көрсетілген уақыттан артық өшірулі. Бұл жағдайда қауіпсіздік бағдарламасының күйі *Тоқтатылған* немесе *Ақау* болып табылады және келесілерден ерекшеленеді: *Іске қосылуда*, *Орындалуда*, немесе *Кідіртілді*.	0 минуттан көбірек.
Қауіпсіздік бағдарламасы іске қосылмаған	Құрылғы көзге көрінеді және қауіпсіздік бағдарламасы құрылғыда орнатылған, бірақ іске қосылмаған.	• Қосқыш өшірулі. • Қосқыш қосулы.

Kaspersky Security Center бағдарламасы белгіленген шарттарды орындау кезінде басқару тобындағы құрылғы күйін автоматты түрде ауыстырып қосуды конфигурациялауға мүмкіндік береді. Белгіленген шарттарды орындау кезінде, клиент құрылғысына келесі күйлердің бірі беріледі: *Критикалық* немесе *Ескерту*. Белгіленген шарттарды орындамаған жағдайда, клиент құрылғысына *ОК* күйі беріледі.

Бір шарттың әртүрлі мәндеріне әртүрлі күйлер сәйкес келуі мүмкін. Мысалы, әдепкі бойынша **3 күннен артық** мәні бар **Дерекқорлар ескірген** шартын ұстанған кезде клиент құрылғысына *Ескерту* күйі, ал **7 күннен артық** мәні бар шартты ұстанған кезде клиент құрылғысына *Критикалық* күйі беріледі.

Kaspersky Security Center бағдарламасын алдыңғы нұсқасынан жаңартып жатсаңыз, *Критикалық* немесе *Ескерту* күйін тағайындау үшін **Дерекқорлар ескірген** шартының мәні өзгермейді.

Құрылғылардың күйлерін ауыстыруды конфигурациялау

Құрылғыға *Критикалық* немесе *Ескерту* күйлерін тағайындау шарттарын өзгерте аласыз.

Құрылғының күйін Критикалық деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Ашылған топтар тізімінде құрылғылардың күйлерін ауыстырып қосуды өзгерткіңіз келетін топтың атауы бар сілтемеден өтіңіз.
3. Пайда болған сипаттар терезесінде **Құрылғының күйі** қойыншасын таңдаңыз.
4. **Критикалық** бөлімін таңдаңыз.
5. **Егер олар көрсетілген болса, Критикалыққа орнатыңыз** блогында құрылғыны *Критикалық* күйіне ауыстырып қосу үшін шартты қосыңыз.

   Алайда, сіз ата-ана саясатында бұғаталмаған параметрлерді өзгерте аласыз.

6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.

9. **ОК** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Критикалық* күйі тағайындалады.

Құрылғының күйін Ескерту деп өзгерту үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Топтардың иерархиясы** бөліміне өтіңіз.
2. Ашылған топтар тізімінде құрылғылардың күйлерін ауыстырып қосуды өзгерткіңіз келетін топтың атауы бар сілтемеден өтіңіз.
3. Пайда болған сипаттар терезесінде **Құрылғының күйі** қойыншасын таңдаңыз.
4. **Ескерту** бөлімін таңдаңыз.
5. **Егер олар көрсетілген болса, Ескертуге орнатыңыз** блогында құрылғыны *Ескерту* күйіне ауыстырып қосу үшін шартты қосыңыз.

   Алайда, сіз ата-ана саясатында бұғатталмаған параметрлерді өзгерте аласыз.

6. Тізімдегі шарттың жанына қосқышты орнатыңыз.
7. Тізімнің жоғарғы сол жақ бұрышындағы **Өңдеу** түймесін басыңыз.
8. Таңдалған шарт үшін өзіңізге қажетті мәнді белгілеңіз.

   Мәндерді барлық шарттар үшін бірдей орнату мүмкін емес.

9. **ОК** түймесін басыңыз.

Белгіленген шарттарды орындамаған жағдайда, басқарылатын құрылғыға *Ескерту* күйі тағайындалады.

Хабарландыруларды жеткізу параметрлерін конфигурациялау

Сіз Kaspersky Security Center бағдарламасында болатын оқиғалар туралы хабарландыруларды конфигурациялай аласыз. Таңдалған хабарландыру тәсіліне байланысты келесі хабарландыру түрлері қолжетімді:

- Электрондық пошта – оқиға болған кезде Kaspersky Security Center бағдарламасы көрсетілген электрондық пошта мекенжайларына хабарландыру жібереді.
- SMS – оқиға болған кезде Kaspersky Security Center бағдарламасы көрсетілген телефон нөмірлеріне хабарландыру жібереді.
- Орындалатын файл – оқиға болған кезде орындалатын файл Басқару серверінде іске қосылады.

Kaspersky Security Center бағдарламасында болған оқиғалар туралы хабарландыруларды жеткізу параметрлерін конфигурациялау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Жалпы қойыншасында Басқару сервері сипаттары терезесі ашылады.

2. **Хабарландыру** бөліміне өтіп, оң жақ тақтадан қажетті хабарландыру тәсілі бар қойыншаны таңдаңыз:

- **Электрондық пошта**

  Электрондық пошта қойыншасында электрондық пошта арқылы оқиғалар туралы хабарландыруларды конфигурациялауға болады.

  Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады.

  SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

  - IPv4 мекенжайы немесе IPv6 мекенжайы;
  - Windows желісіндегі құрылғының атауы (NetBIOS атауы);
  - SMTP сервері DNS атауы.

  SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

  DNS MX іздеуін пайдалану параметрін қоссаңыз, SMTP серверінің бірдей DNS атауы үшін IP мекенжайының бірнеше MX жазбасын қолдана аласыз. Бір DNS атауында, алынған электрондық пошталардың әртүрлі басымдықтары бар бірнеше MX жазбалары болуы мүмкін. Басқару сервері MX жазбаларының басымдылығының өсуі ретімен SMTP серверіне электрондық пошта бойынша хабарландырулар жіберуге тырысады.

  > **DNS MX іздеуін пайдалану** параметрін қосып, TLS параметрін қолдануға рұқсат бермесеңіз, онда хабарландыруларды электрондық пошта бойынша жіберу кезінде қосымша қорғаныс шарасы ретінде сіздің серверлік құрылғыңызда DNSSEC параметрлерін қолдану ұсынылады.

  ESMTP аутентификациясын пайдалану параметрі қосулы болса, сіз **Пайдаланушы аты** және **Құпиясөз** өрістерінде ESMTP аутентификациясы параметрлерін көрсете аласыз. Әдепкі бойынша, параметр таңдалмаған және ESMTP аутентификациясы параметрлері қолжетімді емес.

  SMTP сервері үшін TLS қосылым параметрлерін көрсетуіңізге болады:

  - **TLS пайдаланбау**

  Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

  - **SMTP сервері қолдау көрсетсе, TLS пайдаланыңыз**

  SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

  - **Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз**

  TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

  > Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

  Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз мәнін таңдасаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

Сіз **Сертификаттарды көрсету** сілтемесінен өтіп, TLS қосылымы үшін сертификатты көрсете аласыз:

- SMTP серверінің сертификаты файлын таңдаңыз:

Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

- Клиент сертификаты файлын таңдаңыз:

Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

- X.509 сертификаты:

Сертификаты бар файлды және жеке кілт файлын көрсетуіңіз қажет. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- pkcs12 контейнері:

Сертификат пен сертификаттың жеке кілті бар бір файлды жүктеуіңіз қажет. Файл жүктелген кезде, жеке кілттің шифрсыздау үшін құпиясөзді көрсету керек. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

Тақырып өрісінде электрондық пошта тақырыбын көрсетіңіз. Сіз өрісті бос қалдыра аласыз.

Тақырып үлгісі ашылмалы тізімінен өзіңіздің электрондық хат тақырыбы үшін үлгіні таңдаңыз. Айнымалы, таңдалған үлгіге сәйкес, **Тақырып** өрісінде автоматты түрде көрсетіледі. Сіз бірнеше тақырып үлгісін таңдап, электрондық пошта тақырыбын жасай аласыз.

Жіберушінің электрондық пошта мекенжайы терезесінде электрондық пошта жіберушінің мекенжайын көрсетіңіз. Егер сіз өрісті бос қалдырсаңыз, әдепкі бойынша алушының мекенжайы қолданылады. Жоқ мекенжайды пайдалану ұсынылмайды.

Хабарландыру хабары өрісінде, оқиға туындаған кезде бағдарлама жіберетін оқиға туралы хабарландырудың стандартты мәтіні қамтылған. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер бар. Хабар мәтінін, оқиғаның егжей-тегжейлі деректері бар алмастырылатын параметрлерді қосу арқылы өзгертуге болады.

> Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өткенде, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Тексеру хабарын жіберу түймесін басу арқылы, хабарлардың дұрыс конфигурацияланғанын тексеруге болады: бағдарлама көрсетілген электрондық пошта мекенжайларына мәтіндік хабарлар жібереді.

- SMS

SMS қойыншасында ұялы телефонға түрлі оқиғалар туралы SMS хабарландыруларын жіберуді конфигурациялауға болады. SMS хабарлар пошта шлюзі арқылы жіберіледі.

SMTP серверлері өрісінде пошта серверлерінің мекенжайларын нүктелі үтір арқылы көрсетіңіз. Келесі параметр мәндерін пайдалануыңызға болады:

- IPv4 мекенжайы немесе IPv6 мекенжайы;
- Windows желісіндегі құрылғының атауы (NetBIOS атауы);
- SMTP сервері DNS атауы.

SMTP серверінің порты өрісінде SMTP серверіне қосылу портының нөмірін көрсетіңіз. Әдепкі бойынша 25-порт орнатылған.

ESMTP аутентификациясын пайдалану параметрі қосулы болса, сіз **Пайдаланушы аты** және **Құпиясөз** өрістерінде ESMTP аутентификациясы параметрлерін көрсете аласыз. Әдепкі бойынша, параметр таңдалмаған және ESMTP аутентификациясы параметрлері қолжетімді емес.

SMTP сервері үшін TLS қосылым параметрлерін көрсетуіңізге болады:

- **TLS пайдаланбау**

Электрондық пошта хабарларын шифрлауды өшіргіңіз келсе, осы параметрді таңдауға болады.

- **SMTP сервері қолдау көрсетсе, TLS пайдаланыңыз**

SMTP серверіне қосылу үшін TLS пайдаланғыңыз келсе, бұл параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверін TLS қолданбай қосады.

- **Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз**

TLS түпнұсқалық растамасы параметрлерін пайдаланғыңыз келсе, осы параметрді таңдауға болады. Егер SMTP сервері TLS қолдамаса, Басқару сервері SMTP серверіне қосыла алмайды.

Бұл параметрді SMTP серверімен қосылымды қорғау үшін пайдалану ұсынылады. Осы параметрді таңдасаңыз, TLS қосылымы үшін түпнұсқалық растама параметрлерін орната аласыз.

Әрқашан TLS пайдаланыңыз, сервер сертификатының жарамдылығын тексеріңіз мәнін таңдасаңыз, SMTP серверінің түпнұсқалық растамасы үшін сертификатты көрсетіп, кез келген TLS нұсқасы арқылы немесе тек TLS 1.2 не одан кейінгі нұсқалары арқылы қосылуға рұқсат бергіңіз келетінін таңдай аласыз. Сондай-ақ, SMTP серверінде клиенттің түпнұсқалық растамасы үшін сертификатты көрсете аласыз.

Сертификаттарды көрсету сілтемесінен өту арқылы SMTP сервері сертификатының файлын көрсетуге болады:

Сіз сенімді сертификаттау орталығынан сертификаттар тізімі бар файлды ала аласыз және оны Басқару серверіне жүктей аласыз. Kaspersky Security Center бағдарламасы SMTP серверінің сертификатына сенімді сертификаттау орталығы қол қойғанын тексереді. SMTP серверінің сертификаты сенімді сертификаттау орталығынан алынбаса, Kaspersky Security Center бағдарламасы SMTP серверіне қосыла алмайды.

Алушылар (электрондық пошта мекенжайлары) өрісінде хабарландырулар жіберілетін электрондық пошта мекенжайларын көрсетіңіз. Бұл өрісте бірнеше мекенжайды нүктелі үтір арқылы көрсетуге болады. Хабарландырулар, көрсетілген электрондық пошта мекенжайларымен байланысты нөмірлері бар телефондарға жеткізіледі.

Тақырып өрісінде электрондық пошта тақырыбын көрсетіңіз.

Тақырып үлгісі ашылмалы тізімінен өзіңіздің электрондық хат тақырыбы үшін үлгіні таңдаңыз. Айнымалы, таңдалған үлгіге сәйкес, **Тақырып** өрісінде көрсетіледі. Сіз бірнеше тақырып үлгісін таңдап, электрондық пошта тақырыбын жасай аласыз.

Жіберушінің электрондық пошта мекенжайы: Егер бұл параметр көрсетілмеген болса, онда оның орнына алушының мекенжайы пайдаланылады. Ескерту: Жалған электрондық пошта мекенжайын пайдалану ұсынылмайды терезесінде электрондық пошта жіберушінің мекенжайын көрсетіңіз. Егер сіз өрісті бос қалдырсаңыз, әдепкі бойынша алушының мекенжайы қолданылады. Жоқ мекенжайды пайдалану ұсынылмайды.

SMS хабар алушыларының телефон нөмірлері өрісінде SMS алу үшін ұялы телефон нөмірлерін көрсетіңіз.

Хабарландыру хабары өрісінде, оқиға туындаған кезде бағдарлама жіберетін оқиға туралы хабарландыру мәтінін жазыңыз. Мәтінде оқиғаның атауы, құрылғының атауы және доменнің атауы сияқты алмастырылатын параметрлер болуы мүмкін.

> Хабарландыру мәтінінде пайыз белгішесі (%) болса, хабар жіберілуі үшін, осы пайыз белгішесін қатарынан екі рет көрсету керек. Мысалы, "Орталық процессор жүктемесі 100%%".

Хабарландырулар санының шегін конфигурациялау сілтемесінен өтіп, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

Хабарлардың дұрыс конфигурацияланғанын тексеру үшін **Тексеру хабарын жіберу** түймесін басыңыз: бағдарлама көрсетілген алушыларға мәтіндік хабарлар жібереді.

- **Іске қосылатын орындалатын файл**

  Егер бұл хабарландыру тәсілі таңдалса, енгізу өрісінде оқиға болған кезде қандай бағдарлама іске қосылатынын көрсетуге болады.

  Оқиға пайда болған кезде, орындалатын файл Басқару серверінде іске қосылады өрісінде іске қосылатын файлдың қалтасы мен атауын көрсетіңіз. Файлды көрсетпес бұрын, файлды дайындаңыз және хабарда жіберілетін оқиға туралы мәліметтерді анықтайтын алмастырылатын параметрлерді көрсетіңіз. Көрсетілген қалта мен файл Басқару серверінде болуы керек.

  Хабарландырулар санының шегін конфигурациялау сілтемесінен өткенде, бағдарлама көрсетілген уақыт аралығында жібере алатын хабарландырулардың ең көп санын көрсетуге болады.

3. Қойыншада хабарландыру параметрлерін конфигурациялаңыз.

4. Басқару сервері сипаттары терезесін жабу үшін **OK** түймесін басыңыз.

Сақталған хабарландыруларды жеткізу параметрлері Kaspersky Security Center бағдарламасында болатын барлық оқиғаларға қолданылады.

Оқиғаларды конфигурациялау бөлімінде, Басқару сервері параметрлерінде, саясат параметрлерінде немесе бағдарлама параметрлерінде белгіленген оқиғалар үшін хабарландыруларды жеткізу параметрлерінің мәндерін өзгертуге болады.

Орындалатын файл көмегімен оқиғалар туралы хабарлау

Kaspersky Security Center орындалатын файлды іске қосу арқылы әкімшіге клиент құрылғыларындағы оқиғалар туралы хабарлауға мүмкіндік береді. Орындалатын файлда әкімшіге жіберілетін оқиғаның алмастырылатын параметрлері бар басқа орындалатын файл болуы керек (төмендегі кестені қараңыз).

Оқиғаны сипаттауға арналған алмастырылатын параметрлер

Алмастырылатын параметр	Алмастырылатын параметр сипаттамасы
%SEVERITY%	Оқиғаның маңыздылық деңгейі. Ықтимал мәндер: • **Ақпараттық** • **Ескерту** • **Сәтсіз аяқталды** • **Критикалық**
%COMPUTER%	Оқиға болған құрылғының атауы. Құрылғы атауының максималды ұзындығы - 256 таңба.
%DOMAIN%	Оқиға болған құрылғының домен атауы.

Алмастырылатын параметр	Алмастырылатын параметр сипаттамасы
%EVENT%	Оқиға түрінің атауы. Оқиға түрінің атауының максималды ұзындығы - 50 таңба.
%DESCR%	Оқиғаның сипаттамасы. Максималды сипаттама ұзындығы - 1000 таңба.
%RISE_TIME%	Оқиғаны құру уақыты.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Тапсырманың атауы. Тапсырма атауының максималды ұзындығы - 100 таңба.
%KL_PRODUCT%	Бағдарлама атауы.
%KL_VERSION%	Қолданба нұсқасының нөмірі.
%KLCSAK_EVENT_SEVERITY_NUM%	Оқиғаның маңыздылық деңгейінің коды. Ықтимал мәндер: • 1 – **Ақпараттық**. • 2 – **Ескерту**. • 3 – **Сәтсіздік**. • 4 – **Критикалық**.
%HOST_IP%	Оқиға болған құрылғының IP мекенжайы.
%HOST_CONN_IP%	Оқиға болған құрылғы қосылымының IP мекенжайы.

Мысалы:
Оқиға туралы хабарлау үшін орындалатын файл қолданылады (мысалы, script1.bat), оның ішінде %COMPUTER% алмастырылатын параметрі бар басқа орындалатын файл іске қосылады (мысалы, script2.bat). Оқиға болған кезде әкімші құрылғысында script1.bat файлы іске қосылып, өз кезегінде %COMPUTER% параметрі бар script2.bat файлын іске қосады. Нәтижесінде, әкімші оқиға болған құрылғының атын алады.

Kaspersky хабарландырулары

Бұл бөлімде Kaspersky хабарландыруларын қолдану, конфигурациялау және өшіру тәсілі сипатталған.

Kaspersky хабарландырулары туралы

Kaspersky хабарландырулары бөлімі (**Бақылау және есеп беру** → **Kaspersky хабарландырулары**) Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын бағдарламалар туралы ақпаратты ұсынады. Kaspersky Security Center бағдарламасы бөлімдегі ақпаратты жаңартады, ескірген хабарландыруларды жояды және жаңа ақпаратты қосады.

Kaspersky Security Center тек ағымдағы қосылған Басқару серверіне және осы Басқару серверінің басқарылатын құрылғыларында орнатылған Kaspersky бағдарламаларына қатысты Kaspersky хабарландыруларын ғана көрсетеді. Хабарландырулар Басқару серверінің кез келген түрі (негізгі, қосалқы немесе виртуалды) үшін жеке-жеке көрсетіледі.

Kaspersky хабарландыруларын алу үшін Басқару серверінде интернет қосылымы болуы тиіс.

Хабарландыруларға келесі түрдегі ақпарат кіреді:

- Қауіпсіздікке қатысты хабарландырулар.

Қауіпсіздікке қатысты хабарландырулар сіздің желіңізде орнатылған Kaspersky бағдарламалары өзекті күйде болуына және толығымен жұмыс істеуге жарамды болуына арналған. Хабарландыруларда Kaspersky бағдарламаларына арналған критикалық жаңартулар, табылған осалдықтарға арналған түзетулер және Kaspersky бағдарламаларындағы басқа мәселелерді шешу тәсілдері туралы ақпарат қамтылуы мүмкін. Қауіпсіздікке қатысты хабарландырулар әдепкі бойынша қосылған. Хабарландыруларды алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

Сізге желіні қорғау конфигурациясына сәйкес келетін ақпаратты көрсету үшін, Kaspersky Security Center бағдарламасы деректерді Kaspersky бұлтты серверлеріне жібереді және сіздің желіңізде орнатылған Kaspersky бағдарламаларына қатысты хабарландыруларды ғана алады. Серверлерге жіберілуі мүмкін деректер Kaspersky Security Center Басқару серверін орнату кезінде қабылдайтын Лицензиялық келісімде сипатталған.

- Жарнамалық хабарландырулар.

  Жарнамалық хабарландырулар Kaspersky бағдарламаларыңыз үшін арнайы ұсыныстар туралы ақпаратты, Kaspersky жарнамалары мен жаңалықтарын қамтиды. Жарнамалық хабарландырулар әдепкі бойынша өшірулі. Сіз жаңартулардың осы түрін Kaspersky Security Network (KSN) бағдарламасын қоссаңыз ғана аласыз. Сіз KSN өшіріп, жарнамалық хабарландыруларды өшіре аласыз.

  Желілік құрылғыларыңыз үшін және күнделікті тапсырмаларды орындау үшін пайдалы болуы мүмкін өзекті ақпаратты ғана көруіңіз үшін, Kaspersky Security Center бағдарламасы деректерді Kaspersky бұлтты серверлеріне жіберіп, тиісті хабарландыруларды алады. Серверлерге жіберілуі мүмкін деректер KSN мәлімдемесінің "Өңделетін деректер" бөлімінде сипатталған.

Ақпарат маңыздылық бойынша келесі санаттарға бөлінген:

1. Критикалық ақпарат
2. Маңызды жаңалық
3. Ескерту
4. Ақпараттық хабар

Kaspersky Хабарландырулар бөлімінде жаңа ақпарат пайда болған кезде, Kaspersky Security Center Web Console бағдарламасы хабарландырулардың маңыздылық деңгейіне сәйкес келетін хабарландыру белгісін көрсетеді. Бұл хабарландыруды Kaspersky Хабарландырулар бөлімінде көру үшін белгіні түртуге болады.

Kaspersky хабарландырулар параметрлерін, соның ішінде көргіңіз келетін хабарландыру санаттарын және хабарландыру белгісін көрсету орнын көрсете аласыз.

Kaspersky хабарландыру параметрлерін конфигурациялау

Kaspersky хабарландырулары бөлімінде сіз көргіңіз келетін хабарландырулар санаттарын қоса алғанда, Kaspersky хабарландырулары параметрлерін және хабарландыру белгісін қайда көрсету керектігін көрсете аласыз.

Kaspersky хабарландыруларын конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Kaspersky хабарландырулары** бөліміне өтіңіз.
2. **Параметрлер** сілтемесінен өтіңіз.

   Kaspersky хабарландырулары терезесі ашылады.

3. Келесі параметрлерді белгілеңіз:

   - Көргіңіз келетін хабарландырулардың маңыздылық деңгейін таңдаңыз. Басқа санаттағы хабарландырулар көрсетілмейді.
   - Хабарландыру белгісін көргіңіз келетін орналасуды таңдаңыз. Белгі консольдің барлық бөлімдерінде немесе **Бақылау және есеп беру** бөлімінде және оның бөлікшелерінде көрсетілуі мүмкін.

4. **OK** түймесін басыңыз.

   Kaspersky хабарландырулары параметрлері конфигурацияланған.

Kaspersky хабарландыруларын өшіру

Kaspersky хабарландырулары бөлімі (**Бақылау және есеп беру** → **Kaspersky хабарландырулары**) Kaspersky Security Center нұсқаңыз және басқарылатын құрылғыларға орнатылған басқарылатын бағдарламалар туралы ақпаратты ұсынады. Kaspersky хабарландыруларын алып тұрғыңыз келмесе, бұл функцияны өшіре аласыз.

Kaspersky хабарландырулары екі түрлі ақпаратты қамтиды: қауіпсіздікке қатысты хабарландырулар және жарнамалық хабарландырулар. Сіз әрбір түрдегі хабарландыруларды бөлек өшіре аласыз.

Қауіпсіздікпен байланысты хабарландыруларды өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **Kaspersky хабарландырулары** бөлімін таңдаңыз.
3. Қосқышты **Қауіпсіздікке қатысты хабарландырулар Өшірулі** күйіне ауыстырыңыз.
4. **Сақтау** түймесін басыңыз.

   Kaspersky хабарландырулары өшірулі.

Жарнамалық хабарландырулар әдепкі бойынша өшірулі. Сіз Kaspersky Security Network (KSN) қосқан жағдайда ғана жарнамалық хабарландырулар аласыз. KSN өшіру арқылы хабарландырулардың бұл түрін өшіруге болады.

Хабарландыруларды өшіру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойыншасында **KSN-прокси параметрлері** бөлімін таңдаңыз.
3. **Kaspersky Security Network пайдалану Қосулы** параметрін өшіріңіз.
4. **Сақтау** түймесін басыңыз.

   Хабарландырулар өшірулі.

Табылған қауіптер туралы ақпаратты қарап шығу

Анықтау туралы ақпаратты көрсетуді қосуға немесе өшіруге болады.

*Бас мәзірде **Ескертулер** бөлімінің көрсетілуін қосу немесе өшіру үшін:*

1. Бас мәзірде өз есептік жазбаңыздың параметрлеріне өтіп, **Интерфейс опциялары** тармағын таңдаңыз.
2. Пайда болған **Интерфейс параметрлері** терезесінде **EDR ескертулерін көрсету** параметрін қосыңыз немесе өшіріңіз.
3. **Сақтау** түймесін басыңыз.

Консольде бас мәзірдің **Ескертулер** бөліміндегі **Бақылау және есеп беру** бөлімі көрсетіледі. **Ескертулер** бөлімінде, құрылғыларда табылған қауіптер туралы ақпаратты қарай аласыз. EDR Optimum үшін лицензиялық кілтті қоссаңыз, онда Kaspersky Security Center Web Console бағдарламасы бас мәзірдегі **Ескертулер** бөлікшесін автоматты түрде **Бақылау және есеп беру** бөлімінде көрсетеді. Сондай-ақ, сіз анықтаулар туралы ақпарат көрсетілетін веб-виджетті қоса аласыз.

EDR ескертулерін көрсету опциясын қоспай тұрып, EDR Optimum үшін лицензиялық кілтті қосқаннан кейін ғана, **Ескертулер** ішкі бөлімі автоматты түрде көрсетіледі. Лицензиялық кілтті **EDR ескертулерін көрсету** опциясын қосқаннан кейін қоссаңыз, **Ескертулер** ішкі бөлімі осы опцияны қайта қосқаннан кейін ғана көрсетіледі.

Алерт карточкасында анықталған қауіптер туралы толық ақпаратты дұрыс көрсету үшін Kaspersky Endpoint Agent плагинін және Kaspersky Endpoint Security плагинінің үйлесімді нұсқасын (Kaspersky Endpoint Security for Linux 12.1 немесе одан жоғары нұсқасы, Kaspersky Endpoint Security for Mac 12.1 немесе одан жоғары нұсқасы, Kaspersky Endpoint Security for Windows 12.6 немесе одан жоғары нұсқасы) орнату керек.

Анықтауларды күн және өріс мәндері бойынша сүзгілеу үшін **Сүзгі** мәзірін пайдаланыңыз.

Нысан түрі өрісі келесі мәндердің бірін қамтиды:

- Белгісіз
- Фишингтік сілтеме
- Вирус
- Трояндық бағдарлама
- Зиянды құрал
- Қашықтан басқаруға арналған трояндық бағдарлама
- Құрт
- Басқа бағдарлама
- Жарнамалық бағдарлама

- Порнографиялық бағдарлама
- Қауіпті мұрағатталған бағдарлама
- Қауіпті әрекет

Автоматты жауап өрісі келесі мәндердің бірін қамтиды:

- Зиянды нысан анықталды
- Нысан жойылды
- Нысан емделді
- Нысанды зарарсыздандыру сәтсіз аяқталды
- Нысан карантинге көшірілді
- Құпиясөзбен қорғалған мұрағат анықталды
- Вирус анықталды

Cloud Discovery

Kaspersky Security Center қолданбасы Windows операциялық жүйесімен жұмыс істейтін басқарылатын құрылғыларда бұлттық қызметтерді пайдалануды бақылауға және қажетсіз бұлттық қызметтерге кіруді бұғаттауға мүмкіндік береді. Cloud Discovery пайдаланушылардың браузерлер мен жұмыс үстелі қолданбалары арқылы осы қызметтерге қол жеткізу әрекеттерін бақылайды. Сонымен қатар, ол шифрланбаған қосылымдар арқылы (мысалы, HTTP протоколы бойынша) пайдаланушының бұлттық сервистерге қол жеткізу әрекеттерін бақылайды. Бұл функция бұлттық сервистерді жасырын рұқсатсыз пайдалануды анықтауға және тоқтатуға мүмкіндік береді.

Бұғаттау мүмкіндігі Kaspersky Security Center бағдарламасын Kaspersky Next EDR Optimum немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы лицензиясы арқылы белсендірсеңіз ғана қолжетімді болады.

Бұғаттау мүмкіндігі Kaspersky Endpoint Security 11.2 for Windows және одан жоғары нұсқасын пайдаланған кезде ғана қолжетімді. Қауіпсіздік қолданбасының бұрынғы нұсқалары тек бұлттық сервистерді пайдалануды бақылауға мүмкіндік береді.

Cloud Discovery функциясын қосуға және оны қосу қажет қауіпсіздік саясаттарын немесе профильдерді таңдауға болады. Сондай-ақ, функцияны әрбір қауіпсіздік саясаты немесе профиль үшін бөлек қосуға немесе өшіруге болады. Пайдаланушылардың қолжетімділігін шектегіңіз келетін бұлттық сервистерге қол жеткізуді бұғаттай аласыз.

Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттау үшін келесі шарттар орындалғанын тексеріңіз:

- Сіз Windows жүйесіне арналған Kaspersky Endpoint Security 11.2 немесе одан жоғарырақ нұсқаны пайдаланып жатырсыз. Қауіпсіздік қолданбасының бұрынғы нұсқалары тек бұлттық сервистерді пайдалануды бақылауға мүмкіндік береді.

- Сіз Kaspersky Next лицензиясын сатып алдыңыз, ол қажетсіз бұлттық сервистерге қол жеткізуді бұғаттауға мүмкіндік береді. Қосымша мәліметтер алу үшін Kaspersky Next анықтамасын қараңыз.

Бұлттық қызметтерге қол жеткізудің сәтті және бұғатталған әрекеттері туралы ақпарат Cloud Discovery веб-виджетінде және Cloud Discovery есептерінде көрсетіледі. Веб-виджет әрбір бұлттық сервистің тәуекел деңгейін де көрсетеді. Kaspersky Security Center бұлттық қызметтерді пайдалану туралы ақпаратты қауіпсіздік саясаттарымен немесе ол қосылған саясат профильдерімен қорғалған барлық басқарылатын құрылғылардан алады.

Веб-виджетті пайдаланып, Cloud Discovery функциясын қосу

Cloud Discovery функциясы бұлттық сервистерді пайдалану туралы ақпаратты олар қосылған қауіпсіздік саясаттарымен қорғалған барлық басқарылатын құрылғылардан алады. Cloud Discovery функциясы тек Windows жүйесіне арналған Kaspersky Endpoint Security саясаты үшін қосылуы немесе өшірілуі мүмкін.

Cloud Discovery функциясын қосудың екі жолы бар:

- Cloud Discovery веб-виджеті көмегімен.

- Windows жүйесіне арналған Kaspersky Endpoint Security саясатының сипаттарында.

  Windows жүйесіне арналған Kaspersky Endpoint Security саясат сипаттарындағы Cloud Discovery функциясын қосу жолы туралы толық ақпаратты Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасының Cloud Discovery бөлімінен қараңыз.

Cloud Discovery функциясын тек Windows жүйесіне арналған Kaspersky Endpoint Security саясатының параметрлерінде өшіруге болатынын ескеріңіз.

Cloud Discovery функциясын қосу үшін **Жалпы функциялар: Негізгі функционалдылық** функционалды аймағында **Жазу** рұқсатыңыз болуы керек.

Cloud Discovery веб-виджеті көмегімен Cloud Discovery функциясын қосу үшін:

1. Kaspersky Security Center жүйесін ашыңыз.

2. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.

3. **Cloud Discovery** веб-виджетінде **Қосу** түймесін басыңыз.

   Егер сізде Windows жүйесіне арналған Kaspersky Endpoint Security 12.4 нұсқасы орнатылған болса, Windows жүйесіне арналған Kaspersky Endpoint Security саясатының сипаттарында Cloud Discovery функциясын қосыңыз. Қосымша мәліметтер алу үшін Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасының Cloud Discovery бөлімін қараңыз.

Егер сізде Windows жүйесіне арналған Kaspersky Endpoint Security 12.4 нұсқасынан төмен нұсқасы болса, Windows жүйесіне арналған Kaspersky Endpoint Security плагинін 12.5 нұсқасына дейін жаңартыңыз.

4. Ашылған **Cloud Discovery қызметін қосу** терезесінде функцияны қосқыңыз келетін қауіпсіздік саясаттарын таңдап, **Қосу** түймесін басыңыз.

   Келесі саясат параметрлері автоматты түрде қосылады: **Веб-беттермен өзара әрекет жасау үшін веб-трафикке сценарий енгізу**, **Веб-сеанстарды бақылау** және **Шифрланған қосылымдарды тексеру**.

Cloud Discovery функциясы іске қосылды және веб-виджет бақылау тақтасына қосылды.

Cloud Discovery веб-виджетін бақылау тақтасына қосу

Басқарылатын құрылғыларда бұлтты пайдалануды бақылау үшін **Cloud Discovery** веб-виджетін бақылау тақтасына қосуға болады.

Cloud Discovery веб-виджетін бақылау тақтасына қосу үшін **Жалпы функциялар: Негізгі функционалдылық** функционалды аймағында **Жазу** рұқсаты болуы керек.

Cloud Discovery веб-виджетін бақылау тақтасына қосу үшін:

1. Kaspersky Security Center жүйесін ашыңыз.
2. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.
3. **Веб-виджетті қосу не қалпына келтіру** түймесін басыңыз.
4. Қолжетімді веб-виджеттердің тізімінде **Басқа** санатының жанындағы шеврон белгішесін (>) басыңыз.
5. **Cloud Discovery** веб-виджетін таңдап, **Қосу** түймесін басыңыз.

   Cloud Discovery өшірілсе, веб-виджетті пайдаланып, Cloud Discovery функциясын қосу бөліміндегі нұсқауларды орындаңыз.

Таңдалған веб-виджет бақылау тақтасының соңына қосылады.

Бұлттық сервистерді пайдалану туралы ақпаратты қарау

Cloud Discovery веб-виджеті бұлттық сервистерге қол жеткізу әрекеттері туралы ақпаратты көрсетеді. Веб-виджет әрбір бұлттық сервистің тәуекел деңгейін де көрсетеді. Kaspersky Security Center бұлттық қызметтерді пайдалану туралы ақпаратты олар қосылған қауіпсіздік профильдерімен қорғалған барлық басқарылатын құрылғылардан алады.

Көру алдында мыналарға көз жеткізіңіз:

- Cloud Discovery веб-виджеті мониторинг тақтасына қосылған.
- Cloud Discovery функциясы қосылған.
- **Жалпы функциялар: Негізгі функционалдылық** функционалды аймағында **Оқу** құқығыңыз бар.

Cloud Discovery веб-виджетін көру үшін:

1. Kaspersky Security Center жүйесін ашыңыз.
2. Бағдарламаның негізгі терезесінде **Бақылау және есеп беру** → **Бақылау тақтасы** бөліміне өтіңіз.

   Cloud Discovery веб-виджеті бақылау тақтасында көрсетіледі.
3. **Cloud Discovery** веб-виджетінің сол жағында бұлттық сервистер санатын таңдаңыз.

   Веб-виджеттің оң жағындағы кесте пайдаланушылар жиі қатынасуға тырысатын таңдалған санаттағы бес сервиске дейін көрсетеді. Сәтті және бұғатталған қол жеткізу әрекеттері де ескеріледі.
4. Веб-виджеттің оң жағында қажетті қызметті таңдаңыз.

   Төмендегі кестеде осы сервиске жиі кіретін он құрылғыға дейін көрсетіледі. Бұл кестеде есептердің екі түрін жасауға болады: сәтті кіру әрекеттері туралы есеп және бұғатталған кіру әрекеттері туралы есеп.

   Сондай-ақ, осы кестеде белгілі бір құрылғы үшін бұлттық қызметке кіруді бұғаттай аласыз.

Веб-виджетте сұралған деректер көрсетіледі.

Көрсетілген веб-виджетте келесі әрекеттерді орындауға болады:

- Cloud Discovery есептерін көру үшін **Бақылау және есеп беру** → **Есептер** тармағына өтіңіз.
- Таңдалған бұлттық қызметкер қол жеткізуді бұғаттаңыз немесе оған рұқсат беріңіз.

Бұғаттау мүмкіндігі Kaspersky Security Center бағдарламасын Kaspersky Next EDR Optimum немесе Kaspersky кеңейтілген анықтау және әрекет ету сарапшысы лицензиясы арқылы белсендірсеңіз ғана қолжетімді болады.

Бұғаттау мүмкіндігі Kaspersky Endpoint Security 11.2 for Windows және одан жоғары нұсқасын пайдаланған кезде ғана қолжетімді. Қауіпсіздік қолданбасының бұрынғы нұсқалары тек бұлттық сервистерді пайдалануды бақылауға мүмкіндік береді.

Бұлттық сервистің тәуекел деңгейі

Cloud Discovery әрбір бұлттық сервис үшін тәуекел деңгейін анықтайды. Тәуекел деңгейі ұйымыңыздың қауіпсіздік талаптарына сәйкес келмейтін қызметтерді анықтауға көмектеседі. Мысалы, белгілі бір қызметке кіруді бұғаттау туралы шешім қабылдаған кезде тәуекел деңгейін ескеруіңізге болады.

Тәуекел деңгейі бағалау болып табылады және бұлттық сервис немесе өндіруші сапасы туралы ештеңе айтпайды. Тәуекел деңгейі – Kaspersky сарапшыларының ұсынысы.

Бұлттық қызметтердің тәуекел деңгейлері Cloud Discovery веб-виджетінде және барлық бақыланатын бұлттық қызметтер тізімінде көрсетіледі.

Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттау

Пайдаланушылардың қолжетімділігін шектегіңіз келетін бұлттық сервистерге қол жеткізуді бұғаттай аласыз. Сондай-ақ, бұрын бұғатталған бұлттық сервистерге қол жеткізуге рұқсат бере аласыз.

Мысалы, белгілі бір қызметке қол жеткізуді бұғаттау туралы шешім қабылдағанда тәуекел деңгейін ескеруге болады.

Қауіпсіздік саясаты немесе саясат профилі үшін бұлттық сервистерге қол жеткізуге тыйым салуға немесе рұқсат беруге болады.

Қажетсіз бұлттық сервистерге қол жеткізуді бұғаттаудың екі жолы бар:

- Cloud Discovery веб-виджеті көмегімен.

  Бұл жағдайда сервистерге қол жеткізуді бір-бірден бұғаттай аласыз.

- Windows жүйесіне арналған Kaspersky Endpoint Security саясатының сипаттарында.

  Бұл жағдайда, сервистерге қол жеткізуді бір-бірден немесе бүкіл санатты бірден бұғаттай аласыз.

  Windows жүйесіне арналған Kaspersky Endpoint Security саясат сипаттарындағы Cloud Discovery функциясын қосу жолы туралы толық ақпаратты Windows жүйесіне арналған Kaspersky Endpoint Security анықтамасының Cloud Discovery бөлімінен қараңыз.

Веб-виджеттің көмегімен бұлттық сервисті бұғаттау немесе оған қол жеткізуге рұқсат беру үшін:

1. Cloud Discovery веб-виджетін ашып, қалаған бұлттық сервисті таңдаңыз.
2. **Қызметті ең көп пайдаланатын 10 құрылғы** тақтасында қызметті бұғаттағыңыз немесе рұқсат еткіңіз келетін қауіпсіздік саясатын немесе саясат профилін табыңыз.
3. **Саясаттағы не профильдегі қол жеткізу күйі** бағанындағы тиісті жолақта келесі әрекеттердің бірін орындаңыз:
   - Қызметті бұғаттау үшін ашылмалы тізімнен **Бұғатталған** тармағын таңдаңыз.
   - Қызметке рұқсат беру үшін ашылмалы тізімнен **Рұқсат етілген** тармағын таңдаңыз.
4. **Сақтау** түймесін басыңыз.

Таңдалған қызметке қол жеткізу, қауіпсіздік саясаты немесе саясат профилі арқылы бұғатталған немесе рұқсат етілген.

Kaspersky Security Center Web Console белсенділік журналы

Kaspersky Security Center Web Console белсенділік журналы бағдарламалық жасақтаманың істен шығу себептерін анықтауға көмектеседі. Kaspersky Security Center Web Console істен шыққан жағдайда Kaspersky Техникалық қолдау қызметіне хабарласқан кезде Kaspersky Техникалық қолдау қызметінің мамандары сізден журнал файлдарын сұрауы мүмкін. Бағдарламаны қолдану кезінде Kaspersky Security Center Web Console журнал файлдары <Kaspersky Security Center Web Console орнату қалтасы>/logs қалтасында сақталады. Журнал файлдары Kaspersky Техникалық қолдау қызметінің мамандарына автоматты түрде жіберілмейді.

Kaspersky Security Center Web Console белсенділік журналын қосу үшін,

Kaspersky Security Center Web Console орнату шеберінің **Kaspersky Security Center Web Console байланыс параметрлері** терезесінде **Kaspersky Security Center Web Console әрекеттерін тіркеу пәрменін қосу** жалаушасын қойыңыз.

Журнал файлдары мәтіндік пішімде жазылады.

Журнал файлдарының атаулары -<құрамдас атауы>.<құрылғы атауы>-<файлды тексеру нөмірі>.ЖЖЖЖ-АА-КК пішімінде жазылады, мұндағы.

- <құрамдас атауы> – Kaspersky Security Center құрамдасының атауы немесе Kaspersky Security Center Web Console басқару плагинінің атауы.
- <құрылғы атауы> – құрамдас немесе плагин іске қосылған құрылғының атауы (<құрамдас атауы>).
- <файлды тексеру нөмірі> – <құрылғы атауы> құрылғысында іске қосылған <құрылғы атауы> құрамдасы немесе плагині үшін жасалған журнал файлының нөмірі. Бір күн ішінде бір құрамдас немесе плагин (<құрамдас атауы>) және құрылғы (<құрылғы атауы>) үшін бірнеше журнал файлдарын жасауға болады. Журнал файлының максималды өлшемі 50 МБ. Файлдың максималды өлшеміне жеткенде, жаңа журнал файлы жасалады. Жаңа журнал файлы (<файлды тексеру нөмірі>) 1-ге ұлғайтылады.
- ЖЖЖЖ, АА, және КК – бұл журналдың алғашқы жазбасы жасалған жыл, ай және күн. Жаңа журнал файлы жаңа күн басталған кезде жасалады.

Kaspersky Security Center бағдарламасын басқа шешімдермен біріктіру

Бұл бөлімде Kaspersky Security Center Web Console серверінен Kaspersky Managed Detection and Response сияқты Kaspersky басқа бағдарламасына қатынасуды қалай конфигурациялау керектігі сипатталған. Бұл бөлімде SIEM жүйелеріне экспорттауды қалай конфигурациялау керектігі сипатталған.

Фондық қосылым орнату

Kaspersky Security Center Web Console бағдарламасы өзінің фондық тапсырмаларын орындай алуы үшін сізге Kaspersky Security Center Web Console және Басқару сервері арасында сервисаралық байланыс орнату қажет. Есептік жазбада **Жалпы функциялар: Пайдаланушы құқықтары** функционалды аймағының **Нысанның ACL тізімдерін өзгерту** құқығы болса ғана, бұл қосылымды орнатуға болады.

Kaspersky Endpoint Security for Windows 12.6 плагинін орнатсаңыз немесе Kaspersky Endpoint Security for Windows плагинін 11.7 нұсқасынан төмен нұсқадан жаңартып жатсаңыз және фондық қосылым әлі орнатылмаған болса, фондық қосылымды орнату қажеттігі туралы хабарландыру көрсетіледі. Қызметтің есептік жазбасына **Жалпы функционал: Басқару серверімен операциялар** құқықтарын да ұсыну керек болады.

Фондық қосылым орнату үшін:

1. Бағдарламаның негізгі терезесінде **Параметрлер** → **Біріктіру** бөліміне өтіңіз.
2. **Біріктіру** бөлімінде фондық қосылымды орнату қосқышын **Біріктіру үшін фондық қосылу Қосулы** күйіне ауыстырыңыз.
3. **Фондық қосылымды қосу** бөлімінде **ОК** түймесін басыңыз.

Kaspersky Security Center Web Console веб-консолі мен Басқару сервері арасында фондық қосылым орнатылды. Басқару сервері фондық қосылым үшін есептік жазба жасайды және бұл есептік жазба Kaspersky Security Center басқа бағдарламамен немесе Kaspersky шешімімен өзара әрекеттесуін қолдау үшін қызметтік есептік жазба ретінде пайдаланылады. Бұл қызмет есептік жазбасының атауында NWCSvcUser префиксі бар.

Басқару сервері қауіпсіздік мақсатында 30 күн сайын қызмет есептік жазбасының құпия сөзін автоматты түрде өзгертеді. Қызмет есептік жазбасын қолмен жою мүмкін емес. Басқару сервері бұл есептік жазбаны сервис аралық байланыс өшірілген кезде автоматты түрде жояды. Басқару сервері әрбір Басқару консолі үшін бір қызмет есептік жазбасын жасайды және барлық қызмет есептік жазбаларын ServiceNwcGroup деп аталатын қауіпсіздік тобына тағайындайды. Басқару сервері бұл қауіпсіздік тобын Kaspersky Security Center орнату процесінде автоматты түрде жасайды. Сіз осы қауіпсіздік тобын қолмен жоя алмайсыз.

Оқиғаларды SIEM жүйелеріне экспорттау

Бұл бөлімде оқиғаларды SIEM жүйелеріне экспорттауды қалай конфигурациялау керектігі сипатталған.

Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау

Kaspersky Security Center бағдарламасы конфигурациялауды бір тәсілмен орындауға мүмкіндік береді: Syslog пішімін пайдаланатын кез келген SIEM жүйесіне экспорттау, LEEF және CEF пішімдерін пайдаланатын QRadar, Splunk, ArcSight SIEM жүйелеріне экспорттау немесе оқиғаларды тікелей Kaspersky Security Center дерекқорынан SIEM жүйелеріне экспорттау. Осы сценарий аяқталғаннан кейін, Басқару сервері оқиғаларды автоматты түрде SIEM жүйесіне жібереді.

Алдын ала талаптар

Kaspersky Security Center бағдарламасына оқиғаларды экспорттауды конфигурациялауды бастамас бұрын:

- Оқиғаларды экспорттау әдістері туралы көбірек біліңіз.
- Сізде жүйелік параметрлердің мәндері бар екеніне көз жеткізіңіз.

Сіз осы сценарийдің қадамдарын қалаған тәртіппен орындай аласыз.

Оқиғаларды SIEM жүйесіне экспорттау процесі келесі қадамдардан тұрады:

- **Kaspersky Security Center-ден оқиғаларды алу үшін SIEM жүйесін конфигурациялау**

  Нұсқаулар: Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау.

- **SIEM жүйесіне экспорттағыңыз келетін оқиғаны таңдау:**

  Нұсқаулар:

  - Басқару консолі: Syslog пішімінде экспорттау үшін Kaspersky бағдарламаларының оқиғаларын таңдау, Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау.
  - Kaspersky Security Center Web Console: Syslog пішімінде экспорттау үшін Kaspersky бағдарламаларының оқиғаларын таңдау, Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау.

- **Оқиғаларды SIEM жүйесіне экспорттауды келесі тәсілдердің бірімен конфигурациялау:**

  - TCP, UDP немесе TLS over TCP протоколдарын көрсетіңіз.

    Нұсқаулар:

    - Басқару консолі: Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау.
    - Kaspersky Security Center Web Console: Оқиғаларды SIEM жүйелеріне экспорттауды конфигурациялау.

  - Оқиғаларды тікелей Kaspersky Security Center дерекқорынан экспорттауды пайдалану (жалпыға ортақ көріністер жиынтығы Kaspersky Security Center дерекқорында берілген; осы жалпыға ортақ көріністердің сипаттамасын klakdb.chm құжатынан таба аласыз).

Нәтижелер

Оқиғаларды SIEM жүйесіне экспорттауды конфигурациялағаннан кейін, экспорттағыңыз келетін оқиғаларды таңдаған болсаңыз, экспорт нәтижелерін қарай аласыз.

Алдын ала шарттар

Оқиғаларды Kaspersky Security Center-ге автоматты түрде экспорттауды конфигурациялау кезінде SIEM жүйесінің кейбір параметрлерін көрсету қажет. Kaspersky Security Center конфигурациялауға дайындалу үшін осы параметрлерді ертерек нақтылау ұсынылады.

Оқиғаларды SIEM жүйесіне автоматты түрде экспорттауды конфигурациялау үшін келесі параметрлердің мәндерін білу керек:

- **SIEM жүйелік серверінің мекенжайы**

  Қолданылатын SIEM жүйесі орнатылған сервердің мекенжайы. Бұл мәнді SIEM жүйесінің конфигурацияларында нақтылау керек.

- **SIEM жүйесінің сервер порты**

  Kaspersky Security Center және SIEM жүйесінің сервері арасында қосылым орнатылатын порт нөмірі. Бұл мәнді Kaspersky Security Center конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

- **Протокол**

  Хабарларды Kaspersky Security Center-ден SIEM жүйесіне жіберу үшін қолданылатын протокол. Бұл мәнді Kaspersky Security Center конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

Kaspersky Security Center-дегі оқиғалар туралы

Kaspersky Security Center бағдарламасы, басқарылатын бағдарламаларға орнатылған Kaspersky Басқару сервері мен бағдарламаларының жұмысы барысында орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді. Оқиғалар туралы ақпарат Басқару серверінің дерекқорында сақталады. Сіз осы ақпараты сыртқы SIEM жүйелеріне экспорттай аласыз. Оқиғалар туралы ақпаратты сыртқы SIEM жүйелеріне экспорттау арқасында SIEM жүйелерінің әкімшілері басқарылатын құрылғыларда немесе басқару топтарында орын алған қауіпсіздік жүйелерінің оқиғаларына тез арада ден қоя алатын болады.

Оқиға түрлері

Kaspersky Security Center-де хабарландырулардың келесі түрлері бар:

- Жалпы оқиғалар. Бұл оқиғалар барлық Kaspersky басқарылатын бағдарламаларында туындайды. Мысалы, Вирустық шабуыл жалпы оқиға. Жалпы оқиғалар қатаң белгіленген синтаксис пен семантикаға ие. Жалпы оқиғалар, мысалы, есептер мен мониторинг тақтасында қолданылады.

- Kaspersky басқарылатын бағдарламаларының айрықша оқиғалары. Kaspersky әрбір басқарылатын бағдарламасы өзіндік оқиғалар жиынтығына ие.

Оқиғалар көздері

Оқиғалар келесі бағдарламалар тарапынан жасалуы мүмкін:

- Kaspersky Security Center бағдарламасының құрамдастары:
  - Басқару сервері
  - Желілік агент
  - iOS MDM сервері
- Kaspersky басқарылатын бағдарламалары

  Kaspersky басқарылатын қолданбалары жасайтын оқиғалар туралы қосымша ақпарат тиісті қолданба құжаттамасында келтірілген.

Қолданба жасай алатын оқиғалардың толық тізімі қолданба саясатындағы **Оқиғаларды конфигурациялау** қойындысында келтірілген. Басқару сервері үшін, Басқару серверінің сипаттарындағы оқиғалар тізімін қосымша түрде қарап шығуға болады.

Оқиғаның маңыздылық деңгейі

Әрбір оқиғаның өзіндік маңыздылық деңгейі бар. Туындау шарттарына байланысты, оқиғаға түрлі маңыздылық деңгейлері белгіленуі мүмкін. Оқиғалар маңыздылығының төрт деңгейі бар:

- *Критикалық оқиға* – деректерді жоғалтуға, жұмыстағы ақауға немесе критикалық қатеге әкелуі мүмкін критикалық мәселенің туындағанын білдіретін оқиға.
- *Функционалдық ақау* – бағдарламаның жұмысы немесе рәсімді орындау барысында туындаған күрделі мәселенің, қатенің немесе ақаудың орын алғанын білдіретін оқиға.
- *Ескерту* – міндетті түрде күрделі болып саналмаса да, болашақта мәселенің туындауы мүмкін екенін білдіретін оқиға. Оқиғалар туындағаннан кейін бағдарламаның жұмысы деректерді немесе функционалдық мүмкіндіктерді жоғалтпай қалпына келтіріле алса, осы оқиғалар көбінесе Ескертулерге қатысты болып келеді.
- *Ақпараттық хабарлар* – операцияның сәтті орындалуы, бағдарламаның дұрыс жұмыс істеуі немесе рәсімнің аяқталуы туралы хабарлау мақсатында туындайтын оқиға.

Әрбір оқиға үшін Kaspersky Security Center-де қарап шығуға немесе өзгертуге болатын сақтау уақыты белгіленген. Кейбір оқиғалар Басқару серверінің дерекқорында әдепкі бойынша сақталмайды, себебі олар үшін белгіленген уақыт нөлге тең. Сыртқы жүйелерге, Басқару серверінің дерекқорында кемінде бір күн бойы сақталатын оқиғалар ғана экспортталуы мүмкін.

Оқиғаларды экспорттау туралы

Сіз қауіпсіздік жүйелерінің мониторингін қамтамасыз ететін және әртүрлі шешімдерден деректерді шоғырландыратын ұйымдастырушылық және техникалық деңгейлерде қауіпсіздік мәселелерімен жұмыс істейтін орталықтандырылған жүйелерде оқиғалар экспортын қолдана аласыз. Оларға желілік аппараттық жасақтама мен қолданбалардың оқиғалары мен қауіпсіздік жүйелерінің ескертулерін нақты уақыт режимінде талдауды қамтамасыз ететін SIEM жүйелері, сондай-ақ қауіпсіздікті басқару орталықтары (Security Operation Center, SOC) қатысты болып келеді.

SIEM жүйелері деректерді көптеген көздерден, сонымен қатар желілерден, қауіпсіздік жүйелерінен, серверлерден, дерекқорлардан және қолданбалардан алады. Сондай-ақ, олар өңделген деректерді біріктіру функциясын қамтамасыз ете отырып, сізге критикалық оқиғаларды жіберіп алуға мүмкіндік бермейді. Бұдан бөлек, бұл жүйелер әкімшілерді дереу шешім қабылдауды талап ететін қауіпсіздік жүйесінің мәселелері туралы хабардар ету үшін дабыл сигналдары мен байланысты оқиғаларды автоматты талдауды орындайды. Хабарландырулар индикаторлар тақтасында көрсетілуі немесе бөгде арналар бойынша, мысалы, электрондық пошта арқылы таратылуы мүмкін.

Оқиғаларды Kaspersky Security Center-ден сыртқы SIEM жүйелеріне экспорттау рәсіміне екі тарап қатысады: оқиғаларды жіберуші – Kaspersky Security Center және оқиғаларды алушы – SIEM жүйесі. Оқиғаларды экспорттау сәтті аяқталуы үшін, мұны SIEM жүйесінде де, Kaspersky Security Center-де де конфигурациялау керек. Алдымен қай жағын конфигурациялағаныңыз маңызды емес. Kaspersky Security Center жүйесінде оқиғаларды жіберуді конфигурациялауға, содан кейін SIEM жүйесі арқылы оқиғаларды қабылдауды конфигурациялауға немесе керісінше орындауға болады.

Оқиғаларды Kaspersky Security Center-ден жіберу тәсілдерді

Оқиғаларды Kaspersky Security Center-ден сыртқы жүйелерге жіберудің үш тәсілі бар:

- Оқиғаларды Syslog протоколы бойынша кез келген SIEM жүйесіне жіберу.

  Syslog протоколы бойынша Kaspersky Security Center Басқару серверінде және басқарылатын құрылғыларды орнатылған Kaspersky бағдарламаларында орын алған кез келген оқиғаларды жіберуге болады. Syslog протоколы – хабарларды тіркеудің стандартты протоколы. Сіз осы протоколды оқиғаларды кез келген SIEM жүйесіне экспорттау үшін қолдана аласыз.

  Бұл үшін SIEM жүйесіне жібергіңіз келетін оқиғаларды белгілеу керек. Сіз оқиғаларды Басқару консолі немесе Kaspersky Security Center Web Console) көмегімен белгілей аласыз. SIEM жүйесіне тек белгіленген оқиғалар ғана жіберелетін болады. Сіз ештеңе белгілемеген болсаңыз, ешқандай оқиғалар жіберілмейді.

- Оқиғаларды QRadar, Splunk және ArcSight жүйелеріне CEF және LEEF протоколдары бойынша жіберу.

  CEF және LEEF протоколдарын жалпы оқиғаларды экспорттау үшін қолдануға болады. Оқиғаларды CEF және LEEF протоколдары бойынша экспорттау кезінде, белгіленген экспортталатын оқиғаларды таңдау мүмкіндігіңіз жоқ. Мұның орнына, барлық жалпы оқиғалардың экспорты орындалады. Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға түрлендіру үшін siem_conversion_rules.xml file файлын пайдалану қажет. Бұл файлда Kaspersky Security Center оқиға атрибуттарының тізімі және CEF және LEEF форматындағы оқиғалардың сәйкес атрибуттары бар. Сондай-ақ siem_conversion_rules.xml файлында оқиғаларға сәйкес хабарларды жасау ережелері бар. Бұл файл Kaspersky Security Center тарату жиынтығының құрамына кіреді.

  Syslog протоколынан айырмашылығы, CEF және LEEF протоколдары әмбебап болып саналады. CEF және LEEF протоколдары тиісті SIEM жүйелерге (QRadar, Splunk және ArcSight) арналған. Сол себепті, SIEM жүйесінде келесі протоколдардың бірі бойынша оқиғаларды экспорттауды таңдау кезінде қажетті талдағыш қолданылады.

- Тікелей Kaspersky Security Center дерекқорынан кез келген SIEM жүйесіне.

  Осы оқиғаларды экспорттау тәсілі, оқиғаларды SQL сұрауларының көмегімен дерекқордың көпшілікке қолжетімді көріністерінен тікелей алу үшін қолдануы мүмкін. Сұрау салу нәтижелері .xml файлына сақталады, оны сыртқы жүйеге арналған кіріс деректері ретінде қолдануға болады. Тікелей дерекқордан тек көпшілікке қолжетімді көріністерде қолжетімді оқиғаларды ғана экспорттауға болады.

SIEM жүйесінің оқиғаларды алуы

SIEM жүйесі Kaspersky Security Center-ден алынатын оқиғаларды қабылдауы және дұрыс талдауы тиіс. Бұл үшін SIEM жүйесін конфигурациялауды орындау керек. Конфигурация нақты қолданылатын SIEM жүйесіне байланысты болып келеді. Алайда, барлық SIEM жүйелерінің конфигурацияларында қабылдағыш пен талдағышты конфигурациялау сияқты бірқатар жалпы кезеңдер бар.

Оқиғаларды SIEM жүйесінде экспорттауды конфигурациялау туралы

Оқиғаларды Kaspersky Security Center-ден сыртқы SIEM жүйелеріне экспорттау рәсіміне екі тарап қатысады: оқиғаларды жіберуші – Kaspersky Security Center және оқиғаларды алушы – SIEM жүйесі. Оқиғаларды экспорттау, қолданылатын SIEM жүйесінде және Kaspersky Security Center-де конфигурациялануы керек.

SIEM жүйесінде орындалатын конфигурациялар сіз қолданатын жүйеге байланысты болып келеді. Жалпы жағдайда, алынған хабарларды өрістерге жаю үшін, барлық SIEM жүйелеріне хабар қабылдағышты және қажет болса, хабар талдағышты конфигурациялау керек.

Хабар қабылдағышты конфигурациялау

SIEM жүйесі үшін Kaspersky Security Center жіберетін оқиғаларды қабылдау үшін қабылдағышты конфигурациялау қажет. Жалпы жағдайда, SIEM жүйесінде келесі параметрлерді көрсету керек:

- **Экспорттау протоколы немесе кіріс деректері түрі**

  Бұл хабарлама жіберу протоколы, мысалы, UDP. Kaspersky Security Center-де оқиғаларды жіберу үшін таңдалған протоколды көрсету керек.

- **Порт**

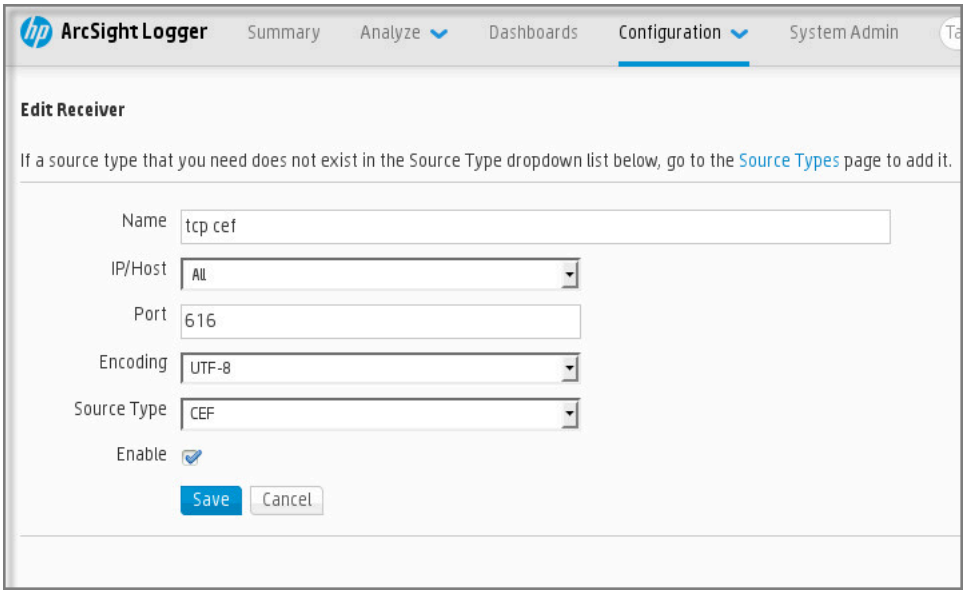
  Kaspersky Security Center-ге қосылуға арналған порт нөмірі. Kaspersky Security Center-де оқиғаларды жіберу үшін таңдалған порт нөмірін көрсету керек.

- **Хабар жіберу протоколы немесе шығыс деректері түрі**

  Оқиғаларды SIEM жүйесіне экспорттау үшін қолданылатын протокол. Бұл келесі стандарттың протоколдардың бірі болуы мүмкін: Syslog, CEF немесе LEEF. SIEM жүйесі аталған протоколға сай келетін оқиғалар талдағышын таңдайды.

Қолданылатын SIEM жүйесіне байланысты, хабар қабылдағыштың қосымша параметрлерін көрсету қажет болуы мүмкін.

Төмендегі суретте, қабылдағышты ArcSight-та конфигурациялау мысалы келтірілген.



Қабылдағышты ArcSight-та конфигурациялау

Хабарлар талдағышы

Экспортталатын оқиғалар SIEM жүйесіне хабарлар түрінде беріледі. Содан соң, оқиғалар туралы ақпарат SIEM жүйесіне тиісінше берілуі үшін, осы хабарларға талдағыш қолданылады. Хабарлар талдағышы SIEM жүйесіне кіріктірілген; ол хабарды хабар идентификаторы, маңыздылық деңгейі, сипаттамасы, параметрлері сияқты өрістерге бөлу үшін қолданылады. Нәтижесінде, SIEM жүйесі Kaspersky Security Center-ден алынған оқиғаларды SIEM жүйесінің дерекқорында сақталатындай етіп өңдеу мүмкіндігіне ие.

SIEM жүйелеріне Syslog пішімінде экспортталатын оқиғаларды таңдау

Оқиғаларды автоматты түрде экспорттауды қосқаннан кейін, сыртқы SIEM жүйесіне қандай оқиғалар экспортталатынын таңдау керек.

Оқиғаларды Syslog пішімінде келесі шарттардың біріне негізделген сыртқы жүйеге экспорттауды конфигурациялауға болады:

- Жалпы оқиғаларды таңдау. Егер сіз саясатта, оқиғаның сипаттарында немесе Басқару сервері сипаттарында экспортталатын оқиғаларды таңдасаңыз, онда осы саясатпен басқарылатын барлық бағдарламаларда орын алған таңдалған оқиғалар SIEM жүйесіне жіберіледі. Егер экспортталатын оқиғалар саясатта таңдалған болса, сіз осы саясатпен басқарылатын жеке бағдарлама үшін оларды қайта анықтай алмайсыз.

- Басқарылатын бағдарлама үшін оқиғаларды таңдау. Егер сіз басқарылатын құрылғыларда орнатылған басқарылатын бағдарлама үшін экспортталатын оқиғаларды таңдасаңыз, онда SIEM жүйесіне тек осы бағдарламада орын алған оқиғалар ғана жіберіледі.

SIEM жүйесіне Syslog пішімінде экспорттау үшін оқиғаларды таңдау туралы

Оқиғаларды автоматты түрде экспорттауды қосқаннан кейін, сыртқы SIEM жүйесіне қандай оқиғалар экспортталатынын таңдау керек.

Оқиғаларды Syslog пішімінде келесі шарттардың біріне негізделген сыртқы жүйеге экспорттауды конфигурациялауға болады:

- Жалпы оқиғаларды таңдау. Егер сіз саясатта, оқиғаның сипаттарында немесе Басқару сервері сипаттарында экспортталатын оқиғаларды таңдасаңыз, онда осы саясатпен басқарылатын барлық бағдарламаларда орын алған таңдалған оқиғалар SIEM жүйесіне жіберіледі. Егер экспортталатын оқиғалар саясатта таңдалған болса, сіз осы саясатпен басқарылатын жеке бағдарлама үшін оларды қайта анықтай алмайсыз.

- Басқарылатын бағдарлама үшін оқиғаларды таңдау. Егер сіз басқарылатын құрылғыларда орнатылған басқарылатын бағдарлама үшін экспортталатын оқиғаларды таңдасаңыз, онда SIEM жүйесіне тек осы бағдарламада орын алған оқиғалар ғана жіберіледі.

Kaspersky бағдарламалары оқиғаларын Syslog пішімінде экспорттау үшін таңдау

Егер сіз басқарылатын құрылғыларда орнатылған белгілі бір басқарылатын бағдарламада болған оқиғаларды экспорттағыңыз келсе, бағдарлама саясатында экспортталатын оқиғаларды таңдаңыз. Бұл жағдайда, белгіленген оқиғалар саясаттың әрекет ету ауқымына кіретін барлық құрылғылардан экспортталады.

Белгілі бір басқарылатын бағдарлама үшін экспортталатын оқиғаларды белгілеу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз.

2. Оқиғаларды белгілеу қажет бағдарлама саясатын таңдаңыз.

   Саясат сипаттары терезесі ашылады.

3. **Оқиғаларды конфигурациялау** бөліміне өту.

4. SIEM жүйесіне экспорттау қажет оқиғалардың жанында жалаушаларды қойыңыз.

5. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** түймесін басыңыз.

   Сондай-ақ, оқиғаға сілтеме арқылы ашылатын **Оқиғаларды тіркеу** бөлімінде SIEM жүйесіне экспортталатын оқиғаны таңдауға болады.

6. Жалауша (✓), сіз SIEM жүйесіне экспорттау үшін белгілеген оқиға немесе оқиғалар үшін **Syslog** бағанында пайда болады.

7. **Сақтау** түймесін басыңыз.

Белгіленген оқиғалар басқарылатын бағдарламадан SIEM жүйесіне экспорттауға дайын.

Белгілі бір басқарылатын құрылғы үшін SIEM жүйесіне қандай оқиғаларды экспорттау керектігін атап өтуге болады. Егер экспортталатын оқиғалар бұған дейін бағдарлама саясатында таңдалған болса, сіз басқарылатын құрылғы үшін таңдалған оқиғаларды қайта анықтай алмайсыз.

Басқарылатын құрылғыға арналған оқиғаларды таңдау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.

   Басқарылатын құрылғылардың тізімі көрсетіледі.

2. Басқарылатын құрылғылар тізімінде қажетті құрылғының атауы бар сілтемеден өтіңіз.

   Таңдалған құрылғы сипаттары терезесі ашылады.

3. **Бағдарламалар** бөліміне өту.

4. Бағдарламалар тізімінде қажетті бағдарламаның атауы бар сілтемеге өтіңіз.

5. **Оқиғаларды конфигурациялау** бөліміне өту.

6. SIEM жүйесіне экспорттау қажет оқиғалардың жанында жалаушаларды қойыңыз.

7. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** түймесін басыңыз.

   Сондай-ақ, оқиғаға сілтеме арқылы ашылатын **Оқиғаларды тіркеу** бөлімінде SIEM жүйесіне экспортталатын оқиғаны таңдауға болады.

8. Жалауша (✓), сіз SIEM жүйесіне экспорттау үшін белгілеген оқиға немесе оқиғалар үшін **Syslog** бағанында пайда болады.

Енді SIEM жүйесіне экспорттауды теңшелген болса, Басқару сервері SIEM жүйесіне таңдалған оқиғаларды жібереді.

Syslog пішімінде экспорттау үшін жалпы оқиғаларды таңдау

Басқару сервері Syslog пішімін пайдаланып, SIEM жүйелеріне экспорттайтын жалпы оқиғаларды белгілей аласыз.

SIEM жүйесіне экспортталатын жалпы оқиғаларды таңдау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер (⚙) белгішесін басыңыз.
   - Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Саясаттар және профильдер** бөліміне өтіңіз, содан соң саясат сілтемесінен өтіңіз.

2. Ашылған терезеде **Оқиғаларды конфигурациялау** қойыншасына өтіңіз.

3. **Syslog көмегімен SIEM жүйесіне экспорттауды белгілеу** түймесін басыңыз.

   Сондай-ақ, оқиғаға сілтеме арқылы ашылатын **Оқиғаларды тіркеу** бөлімінде SIEM жүйесіне экспортталатын оқиғаны таңдауға болады.

4. Жалауша (✓), сіз SIEM жүйесіне экспорттау үшін белгілеген оқиға немесе оқиғалар үшін **Syslog** бағанында пайда болады.

Енді SIEM жүйесіне экспорттауды тоқшелген болса, Басқару сервері SIEM жүйесіне таңдалған оқиғаларды жібереді.

CEF және LEEF пішіміндегі оқиғаларды экспорттау туралы

CEF және LEEF пішімдерін, SIEM жүйесіне жалпы оқиғаларды, сондай-ақ Kaspersky бағдарламалары Басқару серверіне жіберген оқиғаларды экспорттау үшін пайдалануға болады. Экспортталатын оқиғалар жиынтығы алдын ала анықталған, экспортталатын оқиғаларды таңдау мүмкіндігі жоқ. Оқиғаларды SIEM жүйесіне (QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет.

Экспорттау пішімін, сіз қолданатын SIEM жүйесіне байланысты таңдауға болады. Келесі кестеде SIEM жүйелері және оларға сәйкес экспорттау пішімдері келтірілген.

Оқиғаларды SIEM жүйесіне экспорттау пішімдері

SIEM жүйесі	Экспорттау пішімі
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) — IBM Security QRadar SIEM үшін реттелген оқиға пішімі. QRadar платформасы LEEF оқиғаларын ендіріп, анықтап, өңдей алады. LEEF протоколы үшін UTF-8 кодтамасы қолданылуы керек. LEEF протоколы туралы толығырақ ақпаратты IBM Knowledge Center веб-бетінен қараңыз.

- CEF – бұл әртүрлі желілік құрылғылар мен қолданбалардың қауіпсіздік жүйесі ақпаратының үйлесімділігін жақсартатын "ашық журнал" типті басқару стандарты. CEF протоколы, кәсіпорынды басқару жүйелері талдауға арналған деректерді оңай алуы және біріктіруі үшін оқиғалар журналының жалпы пішімін пайдалануға мүмкіндік береді. CEF протоколы үшін UTF-8 кодтамасы қолданылуы керек.

Автоматты түрде экспорттау кезінде Kaspersky Security Center жалпы оқиғаларды SIEM жүйесіне жібереді. Оқиғаларды автоматты түрде экспорттау қосылғаннан кейін бірден басталады. Бұл бөлімде оқиғаларды автоматты түрде экспорттауды қосу рәсімі сипатталған.

Оқиғаларды CEF немесе LEEF форматына түрлендіру

Оқиғаларды SIEM жүйесіне (QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет. Бұл файл Kaspersky Security Center тарату жиынтығының құрамына кіреді.

siem_conversion_rules.xml файлында оқиғаларды CEF және LEEF форматына түрлендіру үшін алдын ала анықталған интерпретациялау ережелері бар. Оқиғаларды интерпретациялаудың қосымша ережелерін пайдаланғыңыз келсе, оларды файлға қолмен қосуға болады.

siem_conversion_rules.xml файлы келесі бөлімдерді қамтиды:

- `<product name="SP_QRADAR" vendor="IBM">`

  Бұл бөлімде оқиғаларды LEEF форматында жасау ережелері бар, оны QRadar SIEM жүйесіне экспорттауға болады.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Бұл бөлімде оқиғаларды CEF форматында жасау ережелері бар, оны ArcSight немесе Splunk SIEM SIEM жүйесіне экспорттауға болады.

Әрбір бөлімде `<common>` ішкі бөлімі бар, ол жерде Kaspersky Security Center оқиға атрибуттары және оқиғалардың LEEF форматындағы тиісті атрибуттары орналасқан. Бұл жалпы атрибуттар экспортталатын оқиғалардың барлық түрі үшін пайдаланылады.

Сондай-ақ әрбір бөлімде `<event>` ішкі бөлімдері бар. Әрбір `<event>` ішкі бөлімінде `<common>` бөліміндегіге қосылатын қосымша атрибуттар бар.

siem_conversion_rules.xml файлына жаңа оқиғаны жасау ережесін қолмен қосуға болады.

Жаңа оқиғаны жасау ережесін қосу үшін:

1. `<product name="SP_QRADAR" vendor="IBM">` немесе `<product name="SP_ARCSIGHT" vendor="HP">` бөліміне жаңа `<event>` ішкі бөлімін қосыңыз, содан кейін қажет болса, қосымша оқиға атрибуттарын көрсетіңіз.

2. Оқиға тек жалпы төлсипаттардан тұрса, `<event>` ішкі бөлімі бос болады.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Syslog пішіміндегі оқиғаларды экспорттау туралы

Syslog пішімін қолдана отырып, басқарылатын құрылғыларда орнатылған Kaspersky Басқару сервері мен басқа да бағдарламаларында орын алған оқиғаларды SIEM жүйелеріне экспорттауға болады.

Syslog – бұл хабарларды тіркеудің стандартты протоколы. Бұл протокол, хабарды құрастыратын бағдарламалық жасақтаманы, хабарлар сақталатын жүйені және хабарлар бойынша талдау мен есептілікті орындайтын бағдарламалық жасақтаманы бөлуге мүмкіндік береді. Әрбір хабарға, хабар құрастырылған бағдарламалық жасақтаманың түрін көрсететін құрылғының коды және маңыздылық деңгейі беріледі.

Syslog пішімі Internet Engineering Task Force жариялаған Request for Comments (RFC) құжаттарымен айқындалады. RFC 5424 стандарты оқиғаларды Kaspersky Security Center-ден сыртқы жүйелерге экспорттау үшін қолданылады.

Kaspersky Security Center-де оқиғаларды Syslog пішімінде сыртқы жүйелерге экспорттауды конфигурациялауға болады.

Экспорттау процесі екі қадамнан тұрады:

1. Оқиғаларды автоматты түрде экспорттауды қосу. Бұл қадамда Kaspersky Security Center бағдарламасы, оқиғалар SIEM жүйесіне жіберілетіндей етіп конфигурацияланады. Автоматты түрде экспорттау қосылғаннан кейін, Kaspersky Security Center-ден оқиғаларды жіберу бірден басталады.

2. Сыртқы жүйеге экспортталатын оқиғаларды таңдау. Бұл қадамда қандай оқиғалардың SIEM жүйесіне экспортталтанын таңдау керек.

Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center конфигурациялау

Оқиғаларды SIEM жүйесіне экспорттау үшін Kaspersky Security Center Web Console веб-консолінен экспорттау процесін реттеу қажет.

Оқиғаларды SIEM жүйесіне (QRadar, ArcSight немесе Splunk) жібермей тұрып, siem_conversion_rules.xml файлында көрсетілген ережелерді пайдалану арқылы Kaspersky Security Center оқиғаларын CEF және LEEF форматындағы оқиғаларға интерпретациялау қажет.

Kaspersky Security Center Web Console веб-консолінен SIEM жүйелеріне экспорттауды конфигурациялау үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **SIEM жүйесіне экспорттау** бөлімін таңдаңыз.

3. **Параметрлер** сілтемесінен өтіңіз.

   Параметрлерді экспорттау бөлімі ашылады.

4. **Параметрлерді экспорттау** бөлімінде параметрлерді көрсетіңіз:

   - **SIEM жүйелік серверінің мекенжайы**

     Қолданылатын SIEM жүйесі орнатылған сервердің мекенжайы. Бұл мәнді SIEM жүйесінің конфигурацияларында нақтылау керек.

- **SIEM жүйелік порты**

  Kaspersky Security Center және SIEM жүйесінің сервері арасында қосылым орнатылатын порт нөмірі. Бұл мәнді Kaspersky Security Center конфигурацияларында және SIEM жүйесіндегі қабылдағыштың конфигурацияларында көрсету қажет.

- **Протокол**

  SIEM жүйесіне хабар жіберу протоколын таңдаңыз. TCP протоколының орнына TCP, UDP немесе TLS таңдауға болады.

  TLS over TCP таңдасаңыз, келесі TLS параметрлерін көрсетіңіз:

  - **Сервердің түпнұсқалық растамасы**

    Сервердің түпнұсқалық растамасы өрісінде **Сенімді сертификаттар** немесе **SHA сәйкестендіру белгілері** мәндерін таңдауға болады:

    - **Сенімді сертификаттар**. Сертификаттардың толық тізбегін (түбірлік сертификатты қоса) сенімді сертификаттау орталығынан (CA) ала аласыз және оны Kaspersky Security Center бағдарламасына жүктей аласыз. Kaspersky Security Center бағдарламасы SIEM жүйесінің сертификаттар тізіміне сенімді сертификаттау орталығы да қол қойғанын тексереді.

      Сенімді сертификатты қосу үшін **Сертификаттау орталығының файлын таңдау** түймесін басып, сертификатты жүктеп алыңыз.

    - **SHA сәйкестендіру белгілері**. Kaspersky Security Center жүйесінде SIEM жүйесінің бүкіл сертификаттар тізбегінің (соның ішінде түбірлік сертификаттың) SHA1 саусақ іздерін көрсетуге болады. SHA1 сәйкестендіру белгісін қосу үшін, оны **Саусақ іздері** өрісіне енгізіп, **Қосу** түймесін басыңыз.

    > **Клиенттік аутентификация қосу** көмегімен Kaspersky Security Center түпнұсқалық растамасы үшін сертификатты жасай аласыз. Осылайша, сіз Kaspersky Security Center шығарған өзіне қол қойылған сертификатты қолданасыз. Бұл жағдайда, SIEM жүйесінің серверінің түпнұсқалық растамасы үшін сенімді сертификатты да, SHA сәйкестендіру белгісін де пайдалануға болады.

  - **Тақырып атауын/Тақырыптың баламалы атауын қосу**

    Субъект атауы – сертификат алуға себеп болған домендік атау. SIEM жүйесі серверінің домендік атауы SIEM жүйесінің сервері сертификаты субъектісінің атына сәйкес келмесе, Kaspersky Security Center бағдарламасы SIEM жүйесінің серверіне қосыла алмайды. Алайда, сертификатта атау өзгерген жағдайда, SIEM жүйесінің сервері өзінің домендік атауын өзгерте алады. Бұл жағдайда, сіз **Тақырып атауын/Тақырыптың баламалы атауын қосу** өрісіндегі субъектілердің аттарын көрсете аласыз. Егер аталған субъектілердің кез келгені SIEM жүйесі сертификаты субъектісінің атына сәйкес келсе, Kaspersky Security Center бағдарламасы SIEM жүйесі серверінің сертификатын тексереді.

  - **Клиенттік аутентификация қосу**

Клиенттің түпнұсқалық растамасы үшін сіз өзіңіздің сертификатыңызды енгізе аласыз немесе оны Kaspersky Security Center бағдарламасында жасай аласыз.

- **Сертификатты енгізу**. Сіз кез келген көзден, мысалы, кез келген сенімді сертификаттау орталығынан алынған сертификатты пайдалана аласыз. Сертификаттың келесі түрлерінің бірін пайдаланып, сертификат пен оның жеке кілтін көрсетуіңіз қажет:

  - **X.509 сертификаты PEM**. Сертификаты бар файлды **Сертификаты бар файл** өрісіне және жеке кілті бар файлды **Кілті бар файл** өрісіне жүктеп салыңыз. Екі файл да бір-біріне тәуелді емес және файлдарды жүктеу реті маңызды емес. Екі файл да жүктелген кезде, **Құпиясөзді немесе сертификатты растау** өрісінде жеке кілтті шифрсыздау үшін құпиясөзді енгізіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

  - **X.509 сертификаты PKCS12**. Сертификат пен оның жеке кілтін қамтитын бір файлды **Сертификаты бар файл** өрісіне жүктеңіз. Файл жүктелгеннен кейін, **Құпиясөзді немесе сертификатты растау** өрісінде жеке кілтті шифрсыздау үшін құпиясөзді көрсетіңіз. Жеке кілт шифрланбаған болса, құпиясөздің мәні бос болуы мүмкін.

- **Кілт жасау**. Сіз Kaspersky Security Center бағдарламасында өзіне қол қойылған сертификатты жасай аласыз. Нәтижесінде, Kaspersky Security Center өзіне қол қойылған сертификатты сақтайды және сіз сертификаттың жария бөлігін немесе SHA1 сәйкестендіру белгісін SIEM жүйесіне жібере аласыз.

- **Деректер пішімі**

  SIEM жүйесінің талаптарына байланысты Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk немесе жүйелік журнал форматтарын таңдай аласыз.

Syslog деректер пішімін таңдасаңыз, мыналарды көрсетуіңіз керек:

- **Хабардың максималды өлшемі, байт**

  SIEM жүйесіне жіберілетін бір хабардың байтындағы максималды өлшемді көрсетіңіз. Әр оқиға бір хабармен беріледі. Егер хабардың нақты ұзындығы көрсетілген мәннен асып кетсе, хабар кесіліп, деректер жоғалуы мүмкін. Хабардың әдепкі өлшемі 2048 байтты құрайды. Бұл өріс **Протокол** өрісінде Syslog пішімін таңдаған болсаңыз ғана қолжетімді.

5. Мұрағатталған оқиғаларды Басқару серверінің дерекқорынан экспорттауға және мұрағатталған оқиғаларды экспорттауды бастағыңыз келетін басталу күнін орнатуға болады:

   a. **Экспорттың басталу күнін орнату** сілтемесіне өтіңіз.

   b. Ашылатын бөлімдегі **Жүйелік оқиғаларды экспорттаудың басталу күні** өрісінде басталу күнін көрсетіңіз.

   c. **OK** түймесін басыңыз.

6. Параметрді **Оқиғаларды SIEM жүйесінің дерекқорына автоматты түрде экспорттау Қосулы** жайғасымына ауыстырып қосыңыз.

7. SIEM жүйесіне қосылым сәтті конфигурацияланғанына көз жеткізу үшін **Байланысты тексеру** түймесін басыңыз.

   SIEM жүйелік серверімен байланыс орнатылып, сынақ оқиғасы жіберіледі. Қосылым күйі көрсетіледі.

Тексеріс TCP және TLS үшін тек TCP протоколдары арқылы жүргізіледі.

8. **Сақтау** түймесін басыңыз.

SIEM жүйесіне экспорттау теңшелді.

Оқиғаларды тікелей дерекқордан экспорттау

Kaspersky Security Center интерфейсін пайдаланбай-ақ, оқиғаларды тікелей Kaspersky Security Center дерекқорынан алуға болады. Тікелей жария көріністерге сұраулар жасауға және олардан оқиғалар туралы деректерді алуға немесе бұрыннан бар жария көріністер негізінде өзіндік көріністер жасауға және қажетті деректерді алу үшін оларға жүгінуге болады.

Жария көріністер

Сізге ыңғайлы болу үшін, Kaspersky Security Center дерекқорында жария көріністер жиынтығы қарастырылған. Жария ұсыныстардың сипаттамасы klakdb.chm құжатында келтірілген.

v_akpub_ev_event жария көрінісі дерекқордағы оқиғалар параметрлеріне сәйкес келетін өрістер жиынтығын қамтиды. klakdb.chm құжатында Kaspersky Security Center-дің басқа нысандарына, мысалы, құрылғыларға, бағдарламаларға, пайдаланушыларға қатысты жария көріністер туралы ақпарат та бар. Сіз бұл ақпаратты сұраулар жасау кезінде пайдалана аласыз.

Бұл бөлімде klsql2 утилитасы арқылы SQL сұрауын жасау нұсқаулары, сондай-ақ осындай сұраудың мысалы берілген.

Сондай-ақ, SQL сұраулары мен дерекқор көріністерін жасау үшін дерекқорлармен жұмыс істеуге арналған кез келген басқа бағдарламаларды пайдалануға болады. Kaspersky Security Center дерекқорына қосылу параметрлерін, мысалы, дананың атауын және дерекқордың атауын қалай қарау керектігі туралы ақпарат тиісті бөлімде берілген.

klsql2 утилитасы арқылы SQL сұрауын жасау

Бұл мақалада klsql2 утилитасын жүктеп алу және пайдалану, сондай-ақ осы утилита арқылы SQL сұрауын жасау туралы нұсқаулар берілген.

klsql2 утилитасын пайдалану үшін:

1. klsql2 утилитасын Kaspersky Security Center орнату қалтасынан табыңыз. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Kaspersky Security Center бағдарламасының ескі нұсқаларына арналған klsql2 утилитасының нұсқаларын пайдаланбаңыз.

2. Кез келген мәтін редакторында .sql кеңейтімі бар файл жасаңыз да, файлды утилитасы бар сол қалтаға салыңыз.

3. .sql файлында қажетті SQL сұрауын теріп, файлды сақтаңыз.

4. Kaspersky Security Center басқару сервері орнатылған құрылғыда .sql файлынан SQL сұрауын іске қосу және нәтижелерді result.xml файлына сақтау үшін келесі пәрменді теріңіз:

```
klsql2 -i src.sql -u <пайдаланушы аты> -p <құпиясөз> -o result.xml
```

мұндағы <пайдаланушы аты> және <құпия сөз> дерекқорға рұқсаты бар пайдаланушы есептік жазбасының есептік деректері болып табылады.

5. Қажет болса, дерекқорға қатынасуға рұқсаты бар пайдаланушының есептік жазбасының атауы мен құпиясөзін енгізіңіз.

6. Жаңадан жасалған result.xml файлдарын ашып, SQL сұрау нәтижелерін қараңыз.

.sql файлын өңдей аласыз және кез келген SQL сұрауын жалпыға жария жасай аласыз. Содан кейін, пәрмен жолындағы пәрменді пайдаланып, SQL сұрауын іске қосып, нәтижелерді файлға сақтауға болады.

klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы

Бұл бөлімде klsql2 утилитасы арқылы жасалған SQL сұрауының мысалы көрсетілген.

Келесі мысалдарда құрылғыларда соңғы жеті күнде орын алған оқиғаларды шығарып алу және пайда болған уақытына байланысты ретімен берілген оқиғалар берілген. Ең соңғы оқиғалар бірінші көрсетіледі.

Microsoft SQL серверінің мысалы:

```
SELECT
  /* оқиға идентификаторы */
  e.nId,

  /* оқиға болған уақыт */
  e.tmRiseTime,

  /* оқиға түрінің ішкі атауы */
  e.strEventType,

  /* оқиғаның көрсетілген атауы */
  e.wstrEventTypeDisplayName,

  /* оқиғаның көрсетілген сипаттамасы */
  e.wstrDescription,

  /* құрылғы орналасқан топтың атауы */
  e.wstrGroupName,

  /* оқиға орын алған құрылғының көрсетілген атауы */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* оқиға орын алған құрылғының IP мекенжайы */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

PostgreSQL мысалы:

```
SELECT
  /* оқиға идентификаторы */
  "e"."nId",

  /* оқиға болған уақыт */
  "e"."tmRiseTime",

  /* оқиға түрінің ішкі атауы */
  "e"."strEventType",

  /* оқиғаның көрсетілген атауы */
  "e"."wstrEventTypeDisplayName",

  /* оқиғаның көрсетілген сипаттамасы */
  "e"."wstrDescription",

  /* оқиғаның көрсетілген сипаттамасы */
  "e"."wstrGroupName",

  /* оқиға орын алған құрылғының көрсетілген атауы */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* оқиға орын алған құрылғының IP мекенжайы */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL немесе MariaDB мысалы:

```
SELECT

  /* оқиға идентификаторы */
  `e`.`nId`,

  /* оқиға болған уақыт */
  `e`.`tmRiseTime`,

  /* оқиға түрінің ішкі атауы */
  `e`.`strEventType`,

  /* оқиғаның көрсетілген атауы */
  `e`.`wstrEventTypeDisplayName`,

  /* оқиғаның көрсетілген сипаттамасы */
  `e`.`wstrDescription`,

  /* құрылғы тобының атауы */
  `e`.`wstrGroupName`,

  /* оқиға орын алған құрылғының көрсетілген атауы */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* оқиға орын алған құрылғының IP мекенжайы */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Kaspersky Security Center дерекқорының атауын қарау

Kaspersky Security Center дерекқорына SQL Server, MySQL немесе MariaDB көмегімен қол жеткізу үшін SQL скрипттер редакторынан оған қосылу мүмкіндігін алу үшін дерекқордың атауын білу қажет.

Kaspersky Security Center дерекқорының атауын көру үшін:

1. Басты мәзірде қажетті Басқару сервері атауының жанындағы параметрлер ( ) белгішесін басыңыз.

   Басқару серверінің сипаттары терезесі ашылады.

2. **Жалпы** қойындысында **Ағымдағы дерекқор мәліметтері** бөлімін таңдаңыз.

Дерекқорының атауы **Дерекқор атауы** өрісінде көрсетілген. SQL сұрауларында дерекқорға қосылу және жүгіну үшін осы дерекқор атауын пайдаланыңыз.

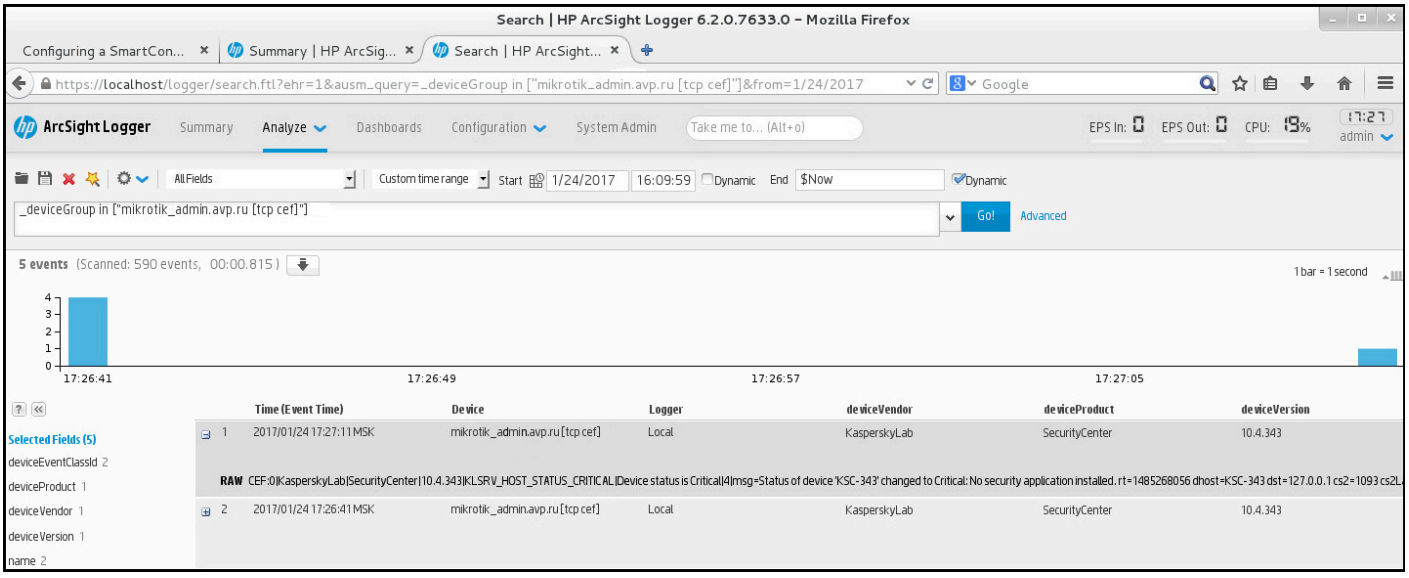
Экспорт нәтижелерін қарау

Экспорттау рәсімі сәтті аяқталғанын білуіңізге болады. Бұл үшін SIEM жүйесі экспортталатын оқиғаларды қамтитын хабарларды алып-алмағанын тексеріңіз.

Kaspersky Security Center-ден жіберілген оқиғаларды SIEM жүйесі алып, дұрыс түсіндірсе, онда екі жақтағы конфигурациялау дұрыс орындалды. Әйтпесе, Kaspersky Security Center және SIEM жүйесінің конфигурациясын тексеріп, қажет болған жағдайда түзетіңіз.

Төменде ArcSight жүйесіне экспортталған оқиғалардың мысалы келтірілген. Мысалы, бірінші оқиға – Басқару серверінің критикалық оқиғасы: *Құрылғының күйі "Критикалық"*.

Экспортталған оқиғалардың көрсетілуі қолданылатын SIEM жүйесіне байланысты.



Оқиғалар мысалы

Kaspersky Security Center Web Console консолімен бұлтты ортада жұмыс істеу

Бұл бөлімде Amazon Web Services, Microsoft Azure және Google Cloud сияқты бұлтты ортада Kaspersky Security Center-ді орналастыруға және қызмет көрсетуге қатысты Kaspersky Security Center Web Console функциялары туралы ақпарат берілген.

Бұлтты ортада жұмыс істеу үшін арнайы лицензия керек. Егер сізде мұндай лицензия болмаса, бұлтты құрылғылармен байланысты интерфейс элементтері көрсетілмейді.

Kaspersky Security Center Web Console веб-консолінде бұлтты ортаны конфигурациялау

Бұлтты ортаны конфигурациялау шеберін пайдаланып Kaspersky Security Center конфигурациялау үшін сізге мыналар қажет:

- Бұлтты орта үшін есептік деректерді көрсетіңіз:
  - Бұлттық сегментте сауалнама өткізу құқығы ұсынылған IAM рөлі немесе бұлттық сегментте сауалнама өткізу құқығы ұсынылған IAM пайдаланушысының есептік жазбасы (Amazon Web Services қызметімен жұмыс істеу үшін);
  - Azure бағдарламасының идентификаторы, құпиясөз және жазылым (Microsoft Azure-мен жұмыс істеу үшін);
  - Google клиентінің электрондық поштасы, жобаның идентификаторы және жабық кілт (Google Cloud-пен жұмыс істеу үшін).
- Орнату пакеттері:
  - Windows үшін Желілік агент
  - Linux үшін Желілік агент
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux веб-плагині
- Кемінде келесілердің бірі:
  - Kaspersky Endpoint Security for Windows орнату пакеті және веб-плагині (ұсынылады)
  - Kaspersky Security for Windows Server орнату пакеті және веб-плагині

Kaspersky Security Center бағдарламасын дайын AMI кескінінен орналастырып жатсаңыз, Басқару серверіне Басқару консолі арқылы алғаш қосылған кезде бұлтты ортаны конфигурациялау шебері автоматты түрде іске қосылады. Сондай-ақ, шеберді кез келген уақытта қолмен іске қоса аласыз.

Бұлтты ортаны конфигурациялау шеберін қолмен іске қосу үшін,

Бағдарламаның негізгі терезесінде **Табу және орналастыру → Орналастыру және тағайындау → Бұлт ортасын конфигурациялау** бөліміне өтіңіз.

Бұлтты ортаны конфигурациялау шебері іске қосылады.

Бұлтты ортаны конфигурациялау уақыты шамамен 15 минут.

1-қадам. Қажетті плагиндер мен орнату пакеттерін тексеру

Егер сізде төменде атап көрсетілген барлық қажетті веб-плагиндер мен орнату пакеттері бар болса, бұл қадам көрсетілмейді.

Бұлтты ортаны конфигурациялау үшін келесі құрамдастардың болуы талап етіледі:

- Орнату пакеттері:
  - Windows үшін Желілік агент
  - Linux үшін Желілік агент
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux веб-плагині
- Кемінде келесілердің бірі:
  - Kaspersky Endpoint Security for Windows орнату пакеті және веб-плагині (ұсынылады)
  - Kaspersky Security for Windows Server орнату пакеті және веб-плагині

    Kaspersky Security for Windows Server орнына Kaspersky Endpoint Security for Windows қолдану ұсынылады.

Kaspersky Security Center бағдарламасы қолданыстағы құрамдастарды автоматты түрде анықтап, жетіспейтінерін атап көрсетеді. **Жүктелетін бағдарламаларды таңдаңыз** түймесін басып, атап көрсетілген құрамдастарды жүктеңіз және плагиндер мен орнату пакеттерін таңдаңыз. Құрамдасты жүктегеннен кейін, сіз жоқ құрамдастар тізімін жаңарту үшін **Жаңарту** түймесін қолдана аласыз.

2-қадам. Қолданбаны лицензиялау

Бұл қадам, AMI BYOL пайдалансаңыз және Kaspersky Security for Virtualization лицензиясы немесе Kaspersky Hybrid Cloud Security лицензиясы арқылы бағдарламаны белсендірмеген жағдайда ғана көрсетіледі.

Лицензиялық кілтті көрсетіп, жалғастыру үшін **Келесі** түймесін басыңыз.

Лицензиялық кілт Басқару серверінің қоймасына қосылған.

Шеберді қайтадан іске қоссаңыз, бұл қадам көрсетілмейді.

3-қадам. Бұлтты ортаны таңдау және түпнұсқалық растама

Бұл бөлімде тек Kaspersky Security Center 12.1 және одан жоғары нұсқасының бағдарламасына қолданылатын функциялар сипатталған.

Келесі параметрлерді белгілеңіз:

- **Бұлтты орта**

  Kaspersky Security Center орналастырылатын бұлтты ортаны таңдаңыз: AWS, Azure немесе Google Cloud.

  Егер сіз бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бір бұлтты ортаны таңдап, содан кейін шеберді қайтадан іске қосыңыз.

- **Қосылым атауы**

  Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

  Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

  Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

Сіз көрсеткен бұлтты ортада түпнұсқалық растама алу үшін есептік деректеріңізді енгізіңіз.

AWS

Бұлттық сегмент түрі ретінде AWS таңдасаңыз, бұлттық сегментте одан әрі сауалнама жүргізу үшін IAM рөлі немесе AWS IAM қатынас кілті керек болады.

- **EC2 үлгісіне тағайындалған AWS IAM рөлі**

  Басқару сервері үшін Қажетті құқықтары бар IAM рөлі бар болса, осы параметрді таңдаңыз.

- **AWS IAM пайдаланушысы**

  Сізде AWS IAM қатынас кілті бар болса, осы параметрді таңдаңыз. Кілт деректеріңізді енгізіңіз:

  - **Қатынас кілтінің идентификаторы**

    IAM қатынас кілті идентификаторы – әріптер мен сандар бірізділігі. IAM пайдаланушысы есептік жазбасын жасау кезінде кілттің идентификаторын алдыңыз.

    Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

  - **Құпия кілт**

    IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

Azure

Бұлттық сегмент түрі ретінде Azure таңдасаңыз, бұлттық сегменттерде сауалнама өткізу үшін келесі қосылым параметрлерін көрсетіңіз:

- **Azure бағдарламасының идентификаторы**

  Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

  Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

- **Azure жазылым идентификаторы**

  Azure порталында жазылым жасадыңыз.

- **Azure бағдарлама құпиясөзі**

  Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

  Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

  Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

- **Azure сақтау орнының есептік жазба атауы**

  Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

- **Azure сақтау орнының қатынас кілті**

  Сіз Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау есептік жазбасын жасаған кезде құпиясөз (кілт) алдыңыз.

  Кілт "Overview of the Azure storage account" бөлімінде, "Keys" бөлікшесінде қолжетімді.

  Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

Google Cloud

Бұлттық сегмент түрі ретінде Google Cloud таңдасаңыз, бұлттық сегменттерде сауалнама өткізу үшін келесі қосылым параметрлерін көрсетіңіз:

- **Клиенттің электрондық пошта мекенжайы**

  Клиенттің электрондық поштасы – бұл сіздің жобаңызды Google Cloud-қа тіркеу үшін пайдаланған электрондық пошта мекенжайы.

- **Жоба идентификаторы**

  Жоба идентификаторы – бұл Google Cloud жобасын тіркеу кезінде алынған идентификатор.

- **Жеке кілт**

  Жеке кілт – бұл жобаны Google Cloud-қа тіркеу кезінде жеке кілт ретінде алынған таңбалар бірізділігі. Қателерді болдырмау үшін осы бірізділікті көшіруге және қоюға болады.

  Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

Көрсетілген қосылым бағдарлама параметрлерінде сақталады.

Бұлтты ортаны конфигурациялау шебері тек бір сегментті көрсетуге мүмкіндік береді. Алдағыда, сіз басқа бұлттық сегменттерді басқару үшін басқа қосылымдарды да көрсете аласыз.

Жалғастыру үшін **Келесі** түймесін басыңыз.

4-қадам. Сегмент сауалнамасы, бұлтты ортамен синхрондауды конфигурациялау және кейінгі әрекеттерді анықтау

Бұл қадамда бұлттық сегменттерде сауалнама өткізу басталады және бұлттық құрылғылар үшін арнайы басқару тобы автоматты түрде құрылады. Сауалнама кезінде табылған құрылғылар осы топқа көшіріледі. Бұлт бойынша сауалнама кестесі конфигурацияланған (әдепкі бойынша 5 минут сайын; сіз осы параметрді кейінірек өзгерте аласыз)

Сондай-ақ, **Бұлтпен синхрондау** автоматты түрде жылжыту ережесі жасалады. Бұлтты ортаны әрбір рет сканерлеген сайын, табылған виртуалды құрылғылар **Басқарылатын құрылғылар\Cloud** тобының ішіндегі тиісті ішкі топқа көшіріледі.

Келесі параметрлерді конфигурациялаңыз:

- **Бұлт құрылымы бар басқару топтарын синхрондау**

  Параметр қосулы болса, онда **Басқарылатын құрылғылар** тобында **Cloud** тобы автоматты түрде жасалып, бұлтты ортада құрылғыларды табу процесі іске қосылады. Бұлтты желіні әрбір рет сканерлеу кезінде табылған даналар мен виртуалды машиналар Cloud тобына көшіріледі. Бұл топтағы басқару ішкі топтарының құрылымы бұлттық сегменттің құрылымына сәйкес келеді (AWS-те қолжетімділік аймақтары мен орналастыру топтары құрылымда көрсетілмеген; Azure-да ішкі желілер құрылымда көрсетілмеген). Бұлтты ортада даналар ретінде анықталмаған құрылғылар **Тағайындалмаған құрылғылар** тобында болады. Мұндай топ құрылымы антивирустық бағдарламаларды топтық орнату тапсырмалары арқылы даналарға орнатуға және әртүрлі топтар үшін әртүрлі саясаттарды конфигурациялауға мүмкіндік береді.

Параметр өшірулі болса, онда **Cloud** тобы да құрылады және бұлтты желідегі құрылғыларды анықтау процесі басталады, алайда топта бұлттық сегментінің құрылымына сәйкес келетін ішкі топтар жасалмайды. Табылған барлық даналар **Cloud** басқару тобында және бір тізімде көрсетіледі. Kaspersky Security Center-мен жұмыс істеу барысында сізге синхрондау қажет болса, онда сіз **Бұлтпен синхрондау** ережесінің сипаттарын өзгертіп, оны қолдана аласыз. Ережені қолдану Cloud тобы ішіндегі топтардың құрылымын бұлттық сегментіңіздің құрылымына сәйкес келетіндей етіп қайта реттейді.

Әдепкі бойынша, параметр өшірулі.

- **Қорғауды жаю**

  Бұл параметр таңдалса, онда шебер қауіпсіздік бағдарламаларын даналарға орнату тапсырмасын жасайды. Шебердің жұмысы аяқталғаннан кейін, бұлттық сегменттеріңіздегі құрылғыларда қорғанысты орналастыру шебері автоматты түрде іске қосылады және сіз бұл құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орната аласыз.

  Kaspersky Security Center өз құралдарының көмегімен орналастыруды орындай алады. Amazon EC2 даналарына немесе Azure виртуалды машиналарына бағдарламаларды орнатуға құқығыңыз болмаса, **қашықтан орнату** тапсырмасын қолмен конфигурациялауға және қажетті құқықтары бар есептік жазбаны көрсетуге болады. Бұл жағдайда, қашықтан орнату тапсырмасы AWS API немесе Azure арқылы анықталған құрылғылар үшін жұмыс істемейді. Бұл тапсырма тек Active Directory сауалнамасы, Windows домендері немесе IP ауқымдары арқылы анықталған құрылғылар үшін ғана жұмыс істейді.

  Бұл параметр таңдалмаса, онда қорғанысты орналастыру шебері іске қосылмайды және қауіпсіздік бағдарламаларын даналарға орнату тапсырмалары жасалмайды. Бұл екі әрекетті де кейінірек қолмен жасауға болады.

Қорғауды жаю параметрін таңдасаңыз, **Құрылғыларды қайта іске қосу** бөлімі қолжетімді болады. Бұл бөлімде, мақсатты құрылғының операциялық жүйесін қайта іске қосу қажет болса, сіз әрекетті таңдауға тиіс боласыз. Бағдарламаларды құрылғыларға орнату барысында операциялық жүйені қайта іске қосу керек болса, даналарды қайта іске қосу қажет пе екенін таңдаңыз:

- **Қайта іске қосуға болмайды**

  Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылмайды.

- **Қайта жүктеу**

  Осы нұсқа таңдалған болса, онда қауіпсіздік бағдарламасы орнатылғаннан кейін, құрылғы қайта іске қосылады.

Жалғастыру үшін **Келесі** түймесін басыңыз.

Google Cloud-ты тек Kaspersky Security Center құралдарының көмегімен орналастыруға болады. Google Cloud-ты таңдасаңыз, **Қорғауды жаю** нұсқасы қолжетімді болмайды.

5-қадам. Саясат пен тапсырмалар жасау үшін бағдарламаны таңдау

Бұл қадам, сізде Kaspersky Endpoint Security for Windows үшін де, Kaspersky Security for Windows Server үшін де орнату пакеттері мен плагиндер болса ғана көрсетіледі. Сізде осы бағдарламалардың біріне ғана арналған плагин мен орнату пакеті болса, бұл қадам өткізіп жіберіледі және Kaspersky Security Center бағдарламасы бұрыннан бар бағдарлама үшін саясат пен тапсырмаларды жасайды.

Саясаты мен тапсырмасын жасау қажет бағдарламасын таңдаңыз:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

6-қадам. Kaspersky Security Center үшін Kaspersky Security Network конфигурациялау

Kaspersky Security Center жұмысы туралы ақпаратты Kaspersky Security Network (KSN) білім базасына беру параметрлерін конфигурациялаңыз. Келесі нұсқалардың бірін таңдаңыз:

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдаймын**

  Kaspersky Security Center және клиент құрылғыларында орнатылған басқарылатын бағдарламалар, олардың жұмысы туралы ақпаратты Kaspersky Security Network қызметіне автоматты режимде жіберетін болады. Kaspersky Security Network-пен ынтымақтастық, вирустар мен қауіптер туралы дерекқорды барынша жылдам жаңартуды қамтамасыз ете отырып, туындаған қауіпсіздік қауіптеріне жауап беру жылдамдығын арттырады.

- **Kaspersky Security Network бағдарламасын пайдалану шарттарын қабылдамаймын**

  Kaspersky Security Center және басқарылатын бағдарламалар өз жұмысы туралы ақпаратты Kaspersky Security Network қызметіне жібермейді.

  Осы параметрді таңдасаңыз, Kaspersky Security Network қызметі өшіріледі.

Kaspersky компаниясы Kaspersky Security Network қызметіне қатысуды ұсынады.

Басқарылатын бағдарламалар үшін KSN ережелері де көрсетілуі мүмкін. Егер сіз Kaspersky Security Network пайдалану шарттарын қабылдасаңыз, басқарылатын бағдарлама деректерді Kaspersky бағдарламасына жібереді. Kaspersky Security Network қызметіне қатысуға келіспесеңіз, басқарылатын қолданба деректерді Kaspersky қызметіне жібермейді. (Бұл параметрді қолданба саясатында кейін өзгерте аласыз.)

Жалғастыру үшін **Келесі** түймесін басыңыз.

7-қадам. Қорғаудың бастапқы конфигурациясын жасау

Сіз жасалған саясаттар мен тапсырмалардың тізімін тексере аласыз.

Саясаттар мен тапсырмалардың жасалуының аяқталғанын күтіп, жалғастыру үшін **Келесі** түймесін басыңыз. Шығу үшін, шебердің соңғы бетінде **Аяқтау** түймесін басыңыз.

Kaspersky Security Center Web Console арқылы желі сегментінде сауалнама өткізу

Желі құрылымы және оның құрамына кіретін құрылғылар туралы ақпаратты Басқару сервері AWS API, Azure API немесе Google API арқылы бұлттық сегменттерде тұрақты түрде сауалнама өткізу арқылы алады. Алынған ақпарат негізінде Kaspersky Security Center басқарылатын құрылғылар мен Басқарылатын құрылғылар қалталарының құрамы мен мазмұнын жаңартады. Құрылғыларды басқару топтарына автоматты түрде жылжытуды конфигурациялаған болсаңыз, желіде анықталған құрылғылар басқару топтарының құрамына қосылады.

Басқару сервері бұлттық сегменттерде сауалнама жүргізе алуы үшін, IAM рөлі немесе IAM пайдаланушысы есептік жазбасы (AWS-те) қамтамасыз ететін тиісті құқықтар, қолданба идентификаторы және құпиясөз (Azure-да) немесе Google клиенті электрондық поштасының мекенжайы, Google жобасының идентификаторы және жеке кілт (Google Cloud-та) керек.

Қосылымдарды қосуға және жоюға, сондай-ақ әрбір бұлттық сегмент үшін сауалнама кестесін конфигурациялауға болады.

Бұлттық сегменттерде сауалнама өткізу үшін қосылымдарды қосу

Бұлттық сегменттерде сауалнама өткізу үшін қосылымды қолжетімділер тізіміне қосу үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **Бұлт** бөліміне өтіңіз.
2. Пайда болған терезеде **Сипаттар** түймесін басыңыз.
3. Пайда болған **Параметрлер** терезесінде **Қосу** түймесін басыңыз.

   Бұлттық сегмент параметрлері терезесі ашылады.
4. Алдағыда бұлттық сегменттерде сауалнама өткізу мақсатымен қолданылатын қосылым үшін бұлтты орта атауын көрсетіңіз:

   - **Бұлтты орта**

     Kaspersky Security Center орналастырылатын бұлтты ортаны таңдаңыз: AWS, Azure немесе Google Cloud.

     Егер сіз бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бір бұлтты ортаны таңдап, содан кейін шеберді қайтадан іске қосыңыз.

   - **Қосылым атауы**

     Қосылым үшін атауын енгізіңіз. Атауы 256 таңбадан аспауы керек. Тек қана Юникод таңбалары рұқсат етіледі.

     Бұл атау бұлтты құрылғылар үшін басқару тобының атауы ретінде де қолданылады.

     Бірнеше бұлтты ортамен жұмыс істеуді жоспарласаңыз, бәлкім "Azure сегменті", "AWS сегменті" немесе "Google сегменті" сияқты қосылым атауына орта атауын қосқыңыз келуі мүмкін.

5. Сіз көрсеткен бұлтты ортада түпнұсқалық растама алу үшін есептік деректеріңізді енгізіңіз.

- Егер сіз AWS таңдаған болсаңыз, келесі параметрлерді көрсетіңіз:

  - **AWS IAM рөлін пайдалану**

    Басқару сервері AWS сервистерімен жұмыс істеуі үшін IAM рөлін жасаған болсаңыз, осы нұсқаны таңдаңыз.

  - **AWS IAM пайдаланушы есептік жазбасының деректемелері**

    Сізде қажетті құқықтары бар IAM пайдаланушысының есептік жазбасы бар болса және сіз кілт идентификаторы мен құпия кілтті енгізе алсаңыз, осы нұсқаны таңдаңыз.

    Сізде AWS IAM пайдаланушы есептік жазбасының деректемелері бар деп көрсетсеңіз, келесіні көрсетіңіз:

    - **Қатынас кілтінің идентификаторы**

      IAM қатынас кілті идентификаторы – әріптер мен сандар бірізділігі. IAM пайдаланушысы есептік жазбасын жасау кезінде кілттің идентификаторын алдыңыз.

      Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

    - **Құпия кілт**

      IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

      Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

      Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

    Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

- Егер сіз Azure таңдаған болсаңыз, келесі параметрлерді көрсетіңіз:

  - **Azure бағдарламасының идентификаторы**

    Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

    Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

  - **Azure жазылым идентификаторы**

    Azure порталында жазылым жасадыңыз.

  - **Azure бағдарлама құпиясөзі**

    Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

    Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

    Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

- **Azure сақтау тіркелгісінің атауы**

  Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

- **Azure сақтау орнының қатынас кілті**

  Сіз Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау есептік жазбасын жасаған кезде құпиясөз (кілт) алдыңыз.

  Кілт "Overview of the Azure storage account" бөлімінде, "Keys" бөлікшесінде қолжетімді.

  Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

Егер сіз Google Cloud таңдаған болсаңыз, келесі параметрлерді көрсетіңіз:

- **Клиенттің электрондық пошта мекенжайы**

  Клиенттің электрондық поштасы – бұл сіздің жобаңызды Google Cloud-қа тіркеу үшін пайдаланған электрондық пошта мекенжайы.

- **Жоба идентификаторы**

  Жоба идентификаторы – бұл Google Cloud жобасын тіркеу кезінде алынған идентификатор.

- **Жеке кілт**

  Жеке кілт – бұл жобаны Google Cloud-қа тіркеу кезінде жеке кілт ретінде алынған таңбалар бірізділігі. Қателерді болдырмау үшін осы бірізділікті көшіруге және қоюға болады.

  Енгізген құпиясөзді қарау үшін **Көрсету** түймесін басып тұрыңыз.

6. Әдепкі бойынша параметрлерді өзгерту үшін **Сауалнама кестесін орнату** түймесін басыңыз.

Қосылым бағдарлама параметрлерінде сақталады.

Жаңа бұлттық сегментте бірінші сауалнама өткізгеннен кейін, **Басқарылатын құрылғылар****Cloud** басқару тобында осы сегментке сай келетін ішкі топ пайда болады.

Дұрыс емес есептік деректерді көрсеткен болсаңыз, онда бұлттық сегменттерде сауалнама өткізу кезінде даналар табылмайды, ал жаңа ішкі топ басқару **Басқарылатын құрылғылар****Cloud** тобында көрсетілмейді.

Бұлттық сегменттерде сауалнама өткізу үшін қосылымды жою

Егер сізге енді бұлттық сегментте сауалнама жүргізудің қажеті болмаса, қолжетімді тізімнен сол сегментке сәйкес келетін қосылымды жоя аласыз. Сондай-ақ, мысалы, бұлттық сегментте сауалнама өткізу құқықтары басқа есептік деректері бар басқа пайдаланушыға ауысқан болса, қосылымды жоюға болады.

Қосылымды жою үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **Бұлт** бөліміне өтіңіз.

2. Пайда болған терезеде **Сипаттар** түймесін басыңыз.

3. Ашылған **Параметрлер** терезесінде жойғыңыз келетін сегменттің атауын басыңыз.

4. **Жою** түймесін басыңыз.

5. Пайда болған терезеде таңдауыңызды растау үшін **ОК** түймесін басыңыз.

Қосылым жойылды. Осы қосылымға сәйкес келетін бұлттық сегменттегі құрылғылар басқару топтарынан автоматты түрде жойылады.

Kaspersky Security Center Web Console арқылы сауалнама өткізу кестесін конфигурациялау

Бұлттық сегменттерде сауалнама өткізу кесте бойынша орындалады. Сіз сауалнама жүргізілетін жиілікті орната аласыз.

Бұлтты ортаны конфигурациялау шеберінің параметрлерінде сауалнама өткізу жиілігі автоматты түрде орнатылады – 5 минутта бір рет. Сіз бұл мәнді кез келген уақытта өзгерте аласыз және басқа кестені белгілей аласыз. Сауалнаманы 5 минутта бір реттен жиі жүргізу ұсынылмайды, себебі бұл API жұмысында қателерге әкелуі мүмкін.

Бұлттық сегменттерде сауалнама өткізу кестесін конфигурациялау үшін:

1. Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **Бұлт** бөліміне өтіңіз.

2. Пайда болған терезеде **Сипаттар** түймесін басыңыз.

3. Ашылған **Параметрлер** терезесінде сауалнама өткізу кестесін конфигурациялағыңыз келетін сегмент атауын басыңыз.

   Бұлттық сегмент параметрлері терезесі ашылады.

4. **Бұлттық сегмент параметрлері** терезесінде **Сауалнама кестесін орнату** түймесін басыңыз.

   Кесте терезесі ашылады.

5. **Кесте** терезесінде келесі параметрлерді көрсетіңіз:

   - **Кесте бойынша іске қосу**

     Сауалнама кестесінің нұсқалары:

     - **N күн сайын**

       Сауалнама белгіленген күн мен уақыттан бастап, көрсетілген күндер аралығымен жүйелі түрде жүргізіледі.

       Әдепкі бойынша, сауалнама ағымдағы жүйелік күн мен уақыттан бастап алты сағат сайын іске қосылып тұрады.

     - N минут сайын

       Сауалнама көрсетілген уақыттан бастап, белгіленген минуттар аралығымен жүйелі түрде жүргізіледі.

       Әдепкі бойынша, сауалнама ағымдағы жүйелік уақыттан бастап бес минут сайын іске қосылады.

     - Апта күндері бойынша

       Сауалнама жүйелі түрде, аптаның көрсетілген күндерінде, көрсетілген уақытта орындалады.

Әдепкі бойынша, сауалнама жұма сайын, сағат 18:00:00-де іске қосылады.

- Ай сайын, таңдалған апталардың көрсетілген күндері

  Сауалнама жүйелі түрде, әр айдың көрсетілген күндерінде, көрсетілген уақытта орындалады.

  Әдепкі бойынша, ай күндері таңдалмаған; әдепкі бойынша басталу уақыты – 18:00:00.

- **Start interval**

  N мәнін (минут немесе күндер үшін) көрсетіңіз.

- **Мына сәттен басталады**

  Бірінші сауалнаманың басталуын көрсетіңіз.

- **Өткізіп алынған тапсырмаларды іске қосу**

  Басқару сервері өшірулі болса немесе сауалнама жоспарланған уақыт ішінде қолжетімді болмаса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастай алады немесе келесі жоспарланған сауалнаманы күте алады.

  Егер бұл параметр қосулы болса, Басқару сервері сауалнаманы қосқаннан кейін бірден бастайды.

  Егер бұл параметр өшірулі болса, Басқару сервері келесі жоспарланған сауалнаманы күтеді.

  Әдепкі бойынша, параметр қосулы.

6. Өзгерістерді сақтаңыз.

Сегмент үшін сауалнама өткізу кестесі конфигурацияланды және сақталды.

Kaspersky Security Center Web Console көмегімен бұлттық сегментте сауалнама өткізу нәтижелерін көру

Сіз бұлттық сегментте сауалнама өткізу нәтижелерін көре аласыз, яғни Басқару сервері басқаратын бұлтты құрылғылардың тізімін көре аласыз.

Бұлттық сегментте сауалнама өткізу нәтижелерін көре аласыз:

Бағдарламаның негізгі терезесінде **Табу және орналастыру** → **Табу** → **Бұлт** бөліміне өтіңіз.

Сауалнама өткізу үшін қолжетімді бұлттық сегменттер көрсетіледі.

Kaspersky Security Center Web Console көмегімен бұлтты құрылғылардың сипаттарын көру

Әр бұлтты құрылғының сипаттарын көруге болады.

Бұлтты құрылғының сипаттарын қарап шығу үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
2. Сипаттарын қарап шығу қажет құрылғыны таңдаңыз.

   Ашылған сипаттар терезесінде **Жалпы** бөлімін таңдаңыз.

3. Қажетті бұлтты құрылғылардың сипаттарын қарап шыққыңыз келсе, сипаттар терезесінен **Жүйе** бөлімін таңдаңыз.

   Сипаттар құрылғының қай бұлтты ортаға жататынына байланысты көрсетіледі.

   AWS құрылғылары үшін келесі сипаттар көрсетіледі:

   - **Құрылғы API көмегімен анықталған** (мәні: **AWS**).
   - **Бұлтты аймақ.**
   - **VPC.**
   - **Бұлтты қолжетімділік аймағы.**
   - **Бұлтты қосалқы желісі.**
   - **Бұлтты орналастыру тобы** (бұл құрылғы, дана орналастыру тобына тиесілі болса көрсетіледі; әйтпесе, сипат көрсетілмейді).

   Azure құрылғылары үшін келесі сипаттар көрсетіледі:

   - **Құрылғы API көмегімен анықталған** (мәні: **Microsoft Azure**).
   - **Бұлтты аймақ.**
   - **Бұлтты қосалқы желісі.**

   Google Cloud құрылғылары үшін келесі сипаттар көрсетіледі:

   - **Құрылғы API көмегімен анықталған** (мәні: **Google Cloud**).
   - **Бұлтты аймақ.**
   - **VPC.**
   - **Бұлтты қолжетімділік аймағы.**
   - **Бұлтты қосалқы желісі.**

Бұлтты сегментпен синхрондау: жылжыту ережесін конфигурациялау

Бұлтты ортаны конфигурациялау кезінде Бұлтты ортамен синхрондау ережесі автоматты түрде жасалады. Бұл ереже әрбір сауалнамада табылған құрылғыларды Тағайындалмаған құрылғылар тобынан Басқарылатын құрылғылар\Cloud тобына автоматты түрде көшіруге мүмкіндік береді, осылайша құрылғылар орталықтан басқару үшін қолжетімді болады. Әдепкі бойынша, ереже жасалғаннан кейін қосулы болады. Сіз ережені қалған уақытта өшіре аласыз, өзгерте аласыз немесе қолдана аласыз.

Бұлтпен синхрондау ережесінің сипаттарын өзгерту және/немесе ережені қолдану үшін:

1. Негізгі терезеде **Табу және орналастыру** → **Орналастыру және тағайындау** → **Жылжыту ережелері** бөліміне өтіңіз.

   Жылжыту ережелері тізімі ашылады.

2. Жылжыту ережелері тізімінен **Бұлтпен синхрондау** тармағын таңдаңыз.

   Ереже сипаттары терезесі ашылады.

3. Қажет болса, **Бұлттық сегменттер** қойындысының **Ереже шарттары** қойындысында келесі параметрлерді көрсетіңіз:

   - **Құрылғы бұлттық сегментте орналасқан**

     Ереже тек таңдалған бұлттық сегментте орналасқан құрылғыларда ғана қолданылады. Әйтпесе, ереже барлық анықталған құрылғыларда қолданылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Қосалқы нысандарды қосу**

     Ереже таңдалған сегменттегі барлық құрылғылар үшін және оның барлық салынған бұлттық бөлімдерінде орындалады. Әйтпесе, ереже түбірлік сегменттегі құрылғылар үшін қолданылады.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Құрылғыларды кірістірілген нысандардан сәйкес қосалқы топтарға жылжыту**

     Параметр қосулы болса, онда құрылғылар салынған нысандардан олардың құрылымына сай келетін ішкі топтарға көшіріледі.

     Параметр қосулы болса, онда құрылғылар салынған нысандардан Cloud ішкі тобының түбіріне көшіріліп, ішкі топтарға бөлінбейді.

     Әдепкі бойынша, параметр қосулы.

   - **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау**

     Жалауша қойылған болса, онда **Басқарылатын құрылғылар\Cloud** топтары құрылымында құрылғы орналасқан бөлімге сай келетін ішкі топ болмаса, онда Kaspersky Security Center осындай ішкі топты құрады. Мысалы, құрылғыларды анықтау барысында жаңа ішкі желі анықталған болса, онда **Басқарылатын құрылғылар\Cloud** тобында осындай атауы бар жаңа топ құрылатын болады.

     Параметр өшірулі болса, онда Kaspersky Security Center ішкі топтарды құрмайды. Мысалы, жаңа ішкі желі желіде сауалнама жүргізу кезінде анықталған болса, онда осындай атауы бар жаңа топ **Басқарылатын құрылғылар\Cloud** тобының астында құрылып, осы ішкі желідегі құрылғылар **Басқарылатын құрылғылар\Cloud** тобына көшірілмейді.

     Әдепкі бойынша, параметр қосулы.

   - **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою**

     Параметр қосулы болса, онда бағдарлама Cloud тобынан ешқандай бұлтты нысандарға сай келмейтін ішкі топтарды жоятын болады.

     Параметр өшірулі болса, онда бұлтты нысандарға сай келмейтін ішкі топтар сақталмайды.

     Әдепкі бойынша, параметр қосулы.

   Бұлтты ортаны конфигурациялау кезінде **Бұлт құрылымы бар басқару топтарын синхрондау** параметрін қосқан болсаңыз, онда **Бұлтпен синхрондау** ережесі **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау** және **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою** қосулы параметрлерімен жасалады.

   Бұлт құрылымы бар басқару топтарын синхрондау параметрін қоспаған болсаңыз, **Бұлтпен синхрондау** ережесі осы өшірулі параметрлермен (жалаушалары алынған) бірге жасалады. Kaspersky Security Center бағдарламасымен жұмыс істеу барысында сізге **Басқарылатын құрылғылар\Cloud** тобының ішкі топтар құрылымы бұлттық сегменттер құрылымына сай келуі қажет болса, ереженің сипаттарында **Жаңадан анықталған құрылғылардың сақтау орындарына қатысты ішкі топтарды жасау** және **Бұлттық сегменттерде сәйкестік жоқ ішкі топтарды жою** параметрлерін қосып, ережені қолданыңыз.

4. **Құрылғы API арқылы табылды** ашылмалы тізімінен мәнді таңдаңыз:

   - **Жоқ**. Құрылғыны AWS, Azure немесе Google API пайдалану арқылы анықтау мүмкін емес, ол бұлттық ортадан тыс немесе бұлттық ортада, бірақ оны белгілі бір себептерге байланысты API арқылы анықтау мүмкін емес.
   - **AWS**. Құрылғы AWS API арқылы табылды, яғни құрылғы AWS бұлтты ортасында орналасқан.
   - **Azure**. Құрылғы Azure API арқылы табылды, яғни құрылғы Azure бұлтты ортасында орналасқан.
   - **Google Cloud**. Құрылғы Google API арқылы табылды, яғни құрылғы Google бұлтты ортасында орналасқан.
   - Көрсетілмеген. Критерий қолданыла алмайды.

5. Қажет болса, басқа бөлімдерде ереженің басқа да сипаттарын конфигурациялаңыз.

Жылжыту ережелері конфигурацияланған.

Azure виртуалды машиналарына бағдарламаларды қашықтан орнату

Microsoft Azure виртуалды машиналарына бағдарламаларды орнату үшін сізде ағымдағы лицензия болуы керек.

Kaspersky Security Center келесі сценарийлерді қолдайды:

- Клиент құрылғысы Azure API көмегімен анықталды; орнату да API арқылы орындалады. Azure API пайдалану тек келесі бағдарламаларды орнатуға болатындығын білдіреді:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Клиент құрылғысы Azure API арқылы анықталады; тарату нүктесі арқылы немесе тарату нүктесі болмаса, жеке орнату пакеттерін пайдаланып қолмен орнатылады. Осылайша, сіз Kaspersky Security Center қолдайтын кез келген бағдарламаны орната аласыз.

Бағдарламаны Azure виртуалды машиналарына қашықтан орнату тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.
2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.
3. Содан кейін, шебердің нұсқауларын орындаңыз:
   a. **Бағдарламаны қашықтан орнату** тапсырма түрін таңдаңыз.
   b. **Орнату пакеттері** бетінде **Microsoft Azure API қашықтан орнатуы** таңдаңыз.

c. Құрылғыларға қатынасу үшін есептік жазбаларды таңдау кезінде бұрыннан бар Azure есептік жазбасын пайдаланыңыз немесе **Қосу** түймесін басып, Azure есептік жазбаңыздың тіркелгі деректерін енгізіңіз:

- **Azure есептік жазбасының атауы**

  Сіз көрсеткен есептік деректер үшін кез келген атауды енгізіңіз. Осы атау, тапсырманы іске қосу үшін есептік жазбалар тізімінде көрсетіледі.

- **Azure бағдарламасының идентификаторы**

  Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

  Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

- **Azure бағдарлама құпиясөзі**

  Azure порталында қолданбаның ID-ін жасау кезінде қолданба идентификаторына құпиясөз алдыңыз.

  Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

d. **Басқарылатын құрылғылар****Cloud** тобындағы қажетті құрылғыларды таңдаңыз.

Шебердің жұмысы аяқталғаннан кейін, бағдарламаны қашықтан орнату тапсырмасы тапсырмалар тізімінде пайда болады.

Бұлтты ДҚБЖ көмегімен Басқару сервері деректерін сақтық көшірмелеу тапсырмасын жасау

Сақтық көшірмелеу тапсырмалары Басқару серверінің тапсырмасына қатысты. Бұлтты ортада (AWS немесе Azure) орналасқан ДҚБЖ пайдаланғыңыз келсе, деректерді сақтық көшірмелеу тапсырмасын жасайсыз.

Басқару серверінің деректерін сақтық көшірмелеу тапсырмасын жасау үшін:

1. Бағдарламаның негізгі терезесінде **Активтер (құрылғылар)** → **Тапсырмалар** бөліміне өтіңіз.

2. **Қосу** түймесін басыңыз.

   Жаңа тапсырма жасау шебері іске қосылады.

3. Шебердің бірінші бетінде, **Бағдарлама** тізімінде **Kaspersky Security Center 15.1** тармағын және **Тапсырма түрі** тізімінде **Басқару сервері деректерінің резервтік қоймасы** тармағын таңдаңыз.

4. Шебердің тиісті бетінде келесі ақпаратты көрсетіңіз:

   - AWS бұлтты ортасында дерекқормен жұмыс істесеңіз:

     - **S3 орнының атауы**

       Деректердің сақтық көшірмесі үшін жасалған S3 орнының атауы.

     - **Қатынас кілтінің идентификаторы**

       Даналар қоймасындағы S3 орнымен жұмыс істеу үшін IAM пайдаланушысының есептік жазбасын жасаған кезде кілттің ID-ін (әріптер мен сандар бірізділігі) алдыңыз.

Бұл өріс, S3 контейнеріне арналған RDS дерекқорын таңдаған кезде қолжетімді.

- **Құпия кілт**

  IAM пайдаланушысының есептік жазбасын жасаған кезде қатынас кілтінің ID-нен алынған құпия кілт.

  Құпия кілттің таңбалары жұлдызшалар түрінде көрсетіледі. Құпия кілтті теруді бастағаннан кейін **Көрсету** түймесі көрсетіледі. Осы түймені басып, енгізілген таңбаларды қарап шығу үшін өзіңізге қажет уақыт бойы ұстап тұрыңыз.

  Авторизациядан өту үшін IAM рөлін емес, AWS IAM қатынас кілтін таңдасаңыз, өріс қолжетімді болады.

- Microsoft Azure бұлтты ортасында дерекқормен жұмыс істесеңіз:

  - **Azure сақтау орнының есептік жазба атауы**

    Kaspersky Security Center-мен жұмыс істеу үшін Azure сақтау орнының есептік жазба атауын жасадыңыз.

  - **Azure жазылым идентификаторы**

    Azure порталында жазылым жасадыңыз.

  - **Azure құпиясөзі**

    Azure порталында бағдарламаның ID-ін жасау кезінде бағдарлама идентификаторына құпиясөз алдыңыз.

    Құпиясөз таңбалары жұлдызшалар түрінде көрсетіледі. Құпиясөзді енгізе бастағаннан кейін, **Көрсету** түймесі көрсетіледі. Енгізілген таңбаларды қарап шығу үшін осы түймені басып тұрыңыз.

  - **Azure бағдарламасының идентификаторы.**

    Сіз Azure порталында осы бағдарлама идентификаторын жасадыңыз.

    Сауалнама жүргізу және басқа мақсаттар үшін Azure порталында тек бір бағдарлама идентификаторын ғана көрсете аласыз. Azure басқа сегментіне сауалнама жүргізу қажет болса, алдымен Azure қолданыстағы қосылымында бірінші сегментті жоюыңыз қажет.

  - **Azure SQL сервері атауы**

    Көздің атауы мен тобы Azure SQL серверінің сипаттарында қолжетімді.

  - **Azure SQL серверінің ресурстық тобы**

    Көздің атауы мен тобы Azure SQL серверінің сипаттарында қолжетімді.

  - **Azure сақтау орнының қатынас кілті**

    "Access Keys" бөлімінде сақтаудың есептік жазбасы сипаттарында қолжетімді. Кез келген кілтті қолдана аласыз (key1 немесе key2).

Тапсырма жасалып, тапсырмалар тізімінде көрсетіледі. **Жасап болған соң, тапсырма туралы мәліметтерді ашу** параметрін қосатын болсаңыз, әдепкі бойынша тапсырма параметрлерін жасағаннан кейін бірден өзгерте аласыз. Егер сіз бұл параметрді қоспасаңыз, тапсырма әдепкі бойынша белгіленген параметр мәндерімен жасалады. Әдепкі бойынша параметр мәндерін кейінірек кез келген уақытта өзгертуге болады.

Клиент құрылғыларын қашықтан диагностикалау

Windows және Linux негізіндегі клиенттік құрылғыларда келесі әрекеттерді қашықтан орындау үшін қашықтағы диагностиканы пайдалануға болады:

- Трассалауды қосу және өшіру, трассалау деңгейін өзгерту және трассалау файлын жүктеу
- Жүйелік ақпарат пен бағдарлама параметрлерін жүктеу
- Оқиғалар журналдарын жүктеу
- Бағдарламадан алынған қоқыс файлын жасау
- Диагностиканы іске қосу және диагностика нәтижелерін жүктеу
- Бағдарламаларды іске қосу, тоқтату және қайта іске қосу

Ақауларды жою үшін клиент құрылғысынан жүктелген оқиғалар журналы мен диагностикалық есептерді пайдалануыңызға болады. Сондай-ақ, Kaspersky Техникалық қолдау қызметіне хабарласатын болсаңыз, онда Kaspersky техникалық қолдау маманы сізден трассалау файлдарын, қоқыс файлдарын, оқиғалар журналын және диагностикалық есептерді Kaspersky талдау мақсатымен клиент құрылғысынан жүктеп алуды сұрауы мүмкін.

Қашықтан диагностикалау терезесін ашу

Windows және Linux негізіндегі клиенттік құрылғыларда қашықтағы диагностиканы орындау үшін алдымен қашықтан диагностикалау терезесін ашу керек.

Қашықтан диагностикалау терезесін ашу үшін:

1. Қашықтан диагностикалау терезесін ашқыңыз келетін құрылғыны таңдау үшін келесі әрекеттердің бірін орындаңыз:
   - Құрылғы басқару тобына тиесілі болса, басты мәзірде **Активтер (құрылғылар)** → **Басқарылатын құрылғылар** бөліміне өтіңіз.
   - Құрылғы тағайындалмаған құрылғылар тобына жататын болса, басты мәзірде **Табу және орналастыру** → **Тағайындалмаған құрылғылар** бөліміне өтіңіз.
2. Қажетті құрылғының атауын басыңыз.
3. Ашылған құрылғының сипаттар терезесінде **Кеңейтілген** бөлімін таңдаңыз.
4. Пайда болған терезеде **Қашықтан диагностикалау** түймесін басыңыз.

   Нәтижесінде, клиент құрылғысының **Қашықтан диагностикалау** терезесі ашылады. Басқару сервер мен клиенттік құрылғы арасында байланыс болмаса, қате туралы хабар пайда болады.

Linux жүйесімен жұмыс істейтін клиенттік құрылғы туралы барлық диагностикалық ақпаратты бірден алу қажет болса, сол құрылғыда collect.sh скриптісін іске қосуға болады.

Бағдарламалар үшін трассалауды қосу және өшіру

xperf трассалауын қоса, бағдарламалар үшін трассалауды қосуға және өшіруге болады.

Трассалауды қосу және өшіру

Қашықтағы құрылғыда трассалауды қосу немесе өшіру үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.
3. Қолданбалар тізімінде трассалауды қосу немесе өшіру қажет қолданбаны таңдаңыз.

   Қашықтан диагностикалау параметрлері тізімі ашады.
4. Трассалауды қосқыңыз келсе:

   a. **Трассирлеу** бөлімінде **Трассирлеуді қосу** түймесін басыңыз.

   b. Ашылған **Трассирлеу деңгейін өзгерту** терезесінде әдепкі бойынша белгіленген мәндерді өзгертпеу ұсынылады. Қажет болса, Техникалық қолдау қызметінің маманы сізді конфигурациялау процесі арқылы өткізеді. Келесі параметрлер қолжетімді:

   - **Трассирлеу деңгейі**

     Трассалау деңгейі, трассалау файлындағы ақпарат құрамын анықтайды.

   - **Айналдыру негізіндегі трассирлеу**

     Бағдарлама трассалау файлының шамадан тыс ұлғаюына жол бермеу үшін трассалау ақпаратын қайта жазады. Трассалау ақпаратын сақтау үшін пайдаланылатын файлдардың ең көп санын және әр файлдың ең үлкен өлшемін көрсетіңіз. Ең үлкен өлшемдегі трассирлеу файлдарының ең көп саны жазылған болса, ең ескі трассирлеу файлы жойылады, осылайша жаңа трассирлеу файлын жазуға болады.

     Бұл параметр тек Kaspersky Endpoint Security үшін ғана қолжетімді.

   c. **Сақтау** түймесін басыңыз.

Трассалау таңдалған бағдарлама үшін қосулы. Кейбір жағдайларда, қауіпсіздік бағдарламасын трассалауды қосу үшін осы бағдарламаны және оның тапсырмасын қайта іске қосу қажет.

Linux жүйесінде жұмыс істейтін клиенттік құрылғыларда желілік агентті жаңарту компонентін трассалау желілік агент параметрлері арқылы реттеледі. Сондықтан Linux арқылы басқарылатын клиенттік құрылғыларда осы компонент үшін **Трассирлеуді қосу** және **Трассирлеу деңгейін өзгерту** параметрлері өшірілген.

5. Таңдалған қолданба үшін трассалауды қосқыңыз келсе, **Трассирлеуді өшіру** түймесін басыңыз.

   Трассалау таңдалған бағдарлама үшін өшірулі.

Xpref трассалауын қосу

Kaspersky Endpoint Security үшін Техникалық қолдау қызметінің мамандары жүйенің өнімділігі туралы ақпарат алу үшін сізден Xperf трассалауын қосуыңызды сұрауы мүмкін.

Xperf трассалауын қосу, орнату немесе өшіру үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.

3. Бағдарламалар тізімінен Kaspersky Endpoint Security for Windows таңдаңыз.

   Kaspersky Endpoint Security for Windows үшін қашықтан диагностикалау параметрлері тізімі көрсетіледі.

4. **Xpref трассирлеу** бөлімінде **Xperf трассирлеуді қосу** түймесін басыңыз.

   Xperf трассалау әлдеқашан қосылған болса, **Xperf трассирлеуді өшіру** түймесі көрсетіледі. Kaspersky Endpoint Security for Windows үшін Xperf трассалауын өшіргіңіз келсе, осы түймені басыңыз.

5. Ашылған **Xperf трассирлеу деңгейін өзгерту** терезесінде, Техникалық қолдау қызметі маманының сұрауына қарай, келесі әрекеттерді орындаңыз:

   a. Трассалау деңгейлерінің бірін таңдаңыз:

   - **Жеңіл деңгей**

     Бұл түрдегі трассирлеу файлы жүйе туралы ақпараттың ықшам өлшемін қамтиды.

     Әдепкі бойынша, осы нұсқа таңдалған.

   - **Күрделі деңгей**

     Бұл түрдегі трассалау файлы *Жеңіл деңгей* типті файлдан да егжей-тегжейлі ақпаратты қамтиды және *жеңіл деңгейлі* трассалау файлындағы ақпарат өнімділікті бағалау үшін жеткіліксіз болса, Техникалық қолдау қызметінің мамандары тарапынан сұралуы мүмкін. *Егжей-тегжейлі деңгейдегі* трассирлеу файлы жабдық, операциялық жүйе туралы ақпаратты, іске қосылған және аяқталған процестер мен бағдарламалардың тізімін, өнімділікті бағалау үшін пайдаланылатын оқиғаларды және Windows жүйесін бағалау құралының оқиғаларын қамтиды.

   b. Xperf трассалау деңгейлерінің бірін таңдаңыз:

   - **Негізгі түрі**

     Бағдарлама трассалау деректерін Kaspersky Endpoint Security бағдарламасы жұмыс істеп тұрған кезде алады.

     Әдепкі бойынша, осы нұсқа таңдалған.

- **Қайта бастау түрі**

  Бағдарлама, басқарылатын құрылғыда операциялық жүйе іске қосылған кезде трассалау деректерін алады. Осы трассалау түрі, жүйенің өнімділігіне әсер ететін мәселе құрылғыны қосқаннан кейін және Kaspersky Endpoint Security іске қосылмай тұрып пайда болған кезде тиімді болады.

Сондай-ақ, трассалау файлының шамадан тыс ұлғаюына жол бермеу үшін **Айналдыру файлының өлшемі, МБ** параметрін қосу ұсынылуы мүмкін. Трассалау файлының ең үлкен өлшемін көрсетіңіз. Файл ең үлкен өлшемге жеткенде, ең ескі трассирлеу файлы жаңа файлмен алмастырылып, қайта жазылады.

c. Ротация файлының өлшемін анықтаңыз.

d. **Сақтау** түймесін басыңыз.

Xperf трассалау қосылған және конфигурацияланған.

6. Kaspersky Endpoint Security for Windows үшін Xperf трассалауын өшіргіңіз келсе, **Xpref трассирлеу** бөліміндегі **Xperf трассирлеуді өшіру** түймесін басыңыз.

   Xpref трассалау өшірулі болса.

Бағдарламаны трассалау файлын жүктеу

Бағдарламаны трассирлеу файлын жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.

3. Қолданбалар тізімінен трассирлеу файлын іске қосқыңыз келетін қолданбаны таңдаңыз.

4. **Трассирлеу** бөлімінде **Файлдарды трассирлеу** түймесін басыңыз.

   Құрылғыны трассирлеу журналдары терезесі ашылып, онда трассалау файлдары тізімі көрсетіледі.

5. Трассалау файлдары тізімінен жүктегіңіз келетін файлды таңдаңыз.

6. Келесі әрекеттердің бірін орындаңыз:

   - **Жүктеп алу** түймесін басып, таңдалған файлды жүктеңіз. Жүктеп салу үшін бір немесе бірнеше файлды таңдауға болады.

   - Таңдалған файлдың бөлігін жүктеңіз:

     a. **Файл бөлігін жүктеп алу** түймесін басыңыз.

     Бірнеше файлды бір уақытта ішінара жүктеу мүмкін емес. Бірнеше трассалау файлын таңдасаңыз, **Файл бөлігін жүктеп алу** түймесі өшіріледі.

b. Ашылған терезеде, өз талаптарыңызға сай жүктеу үшін файлдың аты мен бөлігін көрсетіңіз.

Linux арқылы басқарылатын құрылғылар үшін файл бөлігінің атауын өзгерту мүмкін емес.

c. **Жүктеп алу** түймесін басыңыз.

Таңдалған файл немесе оның бөлігі сіз көрсеткен орналасқан жерге жүктеледі.

Трассалау файлдарын жою

Енді қажет емес трассалау файлдарын жоя беруге болады.

Трассирлеу файлын жою үшін келесі қадамды орындаңыз:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Ашылатын қашықтағы диагностика терезесінде **Оқиға журналдары** бөлімін таңдаңыз.
3. Қай трассалау файлдарын жойғыңыз келетініне байланысты **Файлдарды трассирлеу** бөлімінде **Windows жаңарту журналдары** немесе **Қашықтан орнату журналдары** түймесін басыңыз.

   Windows жаңарту журналдары сілтемесі тек Windows арқылы басқарылатын клиенттік құрылғылар үшін қолжетімді.

   Құрылғыны трассирлеу журналдары терезесі ашылып, онда трассалау файлдары тізімі көрсетіледі.
4. Трассалау файлдары тізімінен жойғыңыз келетін бір немесе бірнеше файлды таңдаңыз.
5. **Жою** түймесін басыңыз.

Таңдалған трассалау файлдары жойылды.

Бағдарламалар параметрлерін жүктеу

Клиент құрылғысынан бағдарлама параметрлерін жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.
3. Клиенттік құрылғыда орнатылған қолданбалардың параметрлері туралы ақпаратты жүктеу үшін **Бағдарлама параметрлері** бөлімінде **Жүктеп алу** түймесін басыңыз.

Ақпараты бар ZIP мұрағаты көрсетілген орынға жүктеледі.

Оқиғалар журналдарын жүктеу

Қашықтағы құрылғыдан оқиғалар журналын жүктеу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінің **Оқиға журналдары** бөлімінде **Барлық құрылғы журналдары** бөлімін таңдаңыз.
3. **Барлық құрылғы журналдары** терезесінде бір немесе бірнеше оқиғалар журналын таңдаңыз.
4. Келесі әрекеттердің бірін орындаңыз:
   - **Бүкіл файлды жүктеп алу** түймесін басып, таңдалған оқиғалар журналын жүктеңіз.
   - Таңдалған оқиғалар журналының бөлігін жүктеңіз:
     a. **Файл бөлігін жүктеп алу** түймесін басыңыз.
     Бірнеше оқиғалар журналын бір уақытта ішінара жүктеп алу мүмкін емес. Бірнеше оқиғалар журналын таңдасаңыз, **Файл бөлігін жүктеп алу** түймесі өшіріледі.
     b. Ашылған терезеде өз талаптарыңызға сай жүктеп алу үшін оқиғалар журналының аты мен бөлігін көрсетіңіз.
     Linux арқылы басқарылатын құрылғылар үшін оқиғалар журналы бөлігінің атауын өзгерту қолжетімді емес.
     c. **Жүктеп алу** түймесін басыңыз.

Таңдалған оқиғалар журналы немесе оның бөлігі көрсетілген жерге жүктеп алынады.

Бағдарламаны іске қосу, тоқтату және қайта іске қосу

Сіз клиент құрылғысында бағдарламаларды іске қоса, тоқтата және қайта іске қоса аласыз.

Бағдарламаны іске қосу, тоқтату және қайта қосу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.
   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.
3. Бағдарламалар тізімінен іске қосқыңыз, тоқтатқыңыз немесе қайта іске қосқыңыз келетін бағдарламаны таңдаңыз.
4. Келесі түймелердің бірін басып, әрекетті таңдаңыз:
   - **Бағдарламаны тоқтату**
     Бұл түйме, бағдарлама қазіргі сәтте іске қосылған болса ғана қолжетімді.

- **Бағдарламаны қайта іске қосу**

  Бұл түйме, бағдарлама қазіргі сәтте іске қосылған болса ғана қолжетімді.

- **Бағдарламаны іске қосу**

  Бұл түйме, бағдарлама қазіргі сәтте іске қосылмаған болса ғана қолжетімді.

Өзіңіз таңдаған әрекетке байланысты, қажетті бағдарлама клиент құрылғысында іске қосылады, тоқтайды немесе қайта іске қосылады.

Желілік агентті қайта іске қоссаңыз, құрылғының Басқару серверімен ағымдағы қосылымы үзілетіні туралы хабар пайда болады.

Kaspersky Security Center Желілік агент қашықтағы диагностикасын іске қосу және нәтижелерді жүктеп алу

Kaspersky Security Center Желілік агент диагностикасын қашықтағы құрылғыда іске қосу және оның нәтижелерін жүктеп алу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Kaspersky бағдарламалары** бөлімін таңдаңыз.

   Бағдарламаларды басқару бөлімінде құрылғыға орнатылған Kaspersky қолданбаларының тізімі көрсетілген.
3. Бағдарламалар тізімінде **Kaspersky Security Center Network Желілік агентін** таңдаңыз.

   Қашықтан диагностикалау параметрлері тізімі ашады.
4. **Диагностикалық есеп** бөлімінде **Диагностиканы іске қосу** түймесін басыңыз.

   Қашықтан диагностикалау процесі іске қосылып, диагностика туралы есеп құрастырылады. Диагностика процесі аяқталғаннан кейін, **Диагностикалық есепті жүктеп алу** түймесі қолжетімді болмайды.
5. Есепті жүктеп алу үшін **Диагностикалық есепті жүктеп алу** түймесін басыңыз.

Есеп көрсетілген орынға жүктеледі.

Бағдарламаны клиент құрылғысында іске қосу

Сізден Kaspersky техникалық қолдау қызметінің маманы сұраса, сізге клиент құрылғысында қолданбаны іске қосу қажет болуы мүмкін. Сізге бағдарламаны осы құрылғыға өз бетіңізше орнатудың қажеті жоқ.

Бағдарламаны клиент құрылғысында іске қосу үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.
2. Қашықтан диагностикалау терезесінде **Қашықтан жұмыс істейтін бағдарламаны іске қосу** бөлімін таңдаңыз.
3. **Бағдарлама файлдары** бөлімінде клиенттік құрылғыда іске қосқыңыз келетін бағдарламамен ZIP мұрағатын таңдау үшін **Шолу** түймесін басыңыз.

ZIP мұрағатында утилита қалтасы болуы керек. Бұл қалта қашықтағы құрылғыда іске қосу үшін орындалатын файлды қамтиды.

Қажет болса, орындалатын файлдың атауын және пәрмен жолы аргументтерін көрсетуге болады. Ол үшін **Қашықтағы құрылғыда жұмыс істейтін мұрағаттағы орындалатын файл** және **Пәрмен жолының аргументтері** өрістерін толтырыңыз.

4. Клиент құрылғысында көрсетілген бағдарламаны іске қосу үшін **Жүктеп салу және іске қосу** түймесін басыңыз.

5. Kaspersky қолдау көрсету қызметі өкілінің нұсқауларын орындаңыз.

Бағдарламадан алынған қоқыс файлын жасау

Бағдарламадан алынған қоқыс файлы белгілі бір уақытта клиент құрылғысында жұмыс істейтін бағдарламаның параметрлерін көруге мүмкіндік береді. Бұл файлда бағдарлама үшін жүктелген модульдер туралы ақпарат та бар.

Linux негізіндегі құрылғылардан дамп файлдарын алуға қолдау көрсетілмейді.

Қашықтағы диагностика арқылы дамп файлдарын алу үшін kldumper утилитасы қолданылады. Бұл утилита техникалық қолдау қызметі мамандарының сұрауы бойынша Kaspersky қолданбалары процестерінің қоқыс файлдарын алуға арналған. kldumper утилитасын пайдалану талаптары туралы толық ақпарат Kaspersky Security Center білім қорында берілген.

Бағдарламаға арналған қоқыс файлын жасау үшін:

1. Клиент құрылғысын қашықтан диагностикалау утилитасын ашыңыз.

2. Қашықтан диагностикалау терезесінде **Қашықтан жұмыс істейтін бағдарламаны іске қосу** бөлімін таңдаңыз.

3. **Процестің дамп файлын жасау** бөлімінде қоқыс жасағыңыз келетін бағдарламаның орындалатын файлын көрсетіңіз.

4. **Дамп файлын жүктеп алу** түймесін басыңыз.

   Көрсетілген бағдарлама үшін дамп файлы бар мұрағат жүктелді.

   Көрсетілген бағдарлама клиент құрылғысында жұмыс істемесе, жүктелген мұрағаттағы "result" қалтасы бос болады.

   Көрсетілген қолданба жұмыс істеп тұрса, бірақ жүктеп алу қатемен сәтсіз аяқталса немесе жүктеп алынған мұрағаттағы "нәтиже" қалтасы бос болса, Kaspersky Security Center білім қорын қараңыз.

Linux операциялық жүйесі бар клиенттік құрылғыда қашықтағы диагностиканы іске қосу

Kaspersky Security Center жүйесі клиенттік құрылғыдан негізгі диагностикалық ақпаратты жүктеп алуға мүмкіндік береді. Бұған қоса Kaspersky бағдарламасының collect.sh скриптісін пайдаланып, Linux операциялық жүйесімен жұмыс істейтін құрылғы туралы диагностикалық ақпаратты алуға болады. Бұл скрипт диагностикалануы қажет Linux негізіндегі клиент құрылғысында іске қосылады, содан кейін диагностикалық ақпараты, осы құрылғы туралы жүйелік ақпараты бар файлды, қолданбалардың трассалау файлдарын, құрылғы журналдарын және төтенше жағдайда тоқтатылатын қолданбаларға арналған дамп файлын жасайды.

Linux операциялық жүйесімен жұмыс істейтін клиенттік құрылғы туралы барлық диагностикалық ақпаратты дереу алу үшін collect.sh скриптісін пайдалану ұсынылады. Егер диагностикалық ақпаратты Kaspersky Security Center арқылы қашықтан жүктеп алсаңыз, қашықтағы диагностика интерфейсінің барлық бөлімдерін өтуіңіз керек. Оған қоса Linux операциялық жүйесі бар құрылғының диагностикалық ақпараты толық алынбауы мүмкін.

Диагностикалық ақпараты бар жасалған файлды Kaspersky техникалық қолдау қызметіне жіберу қажет болса, файлды жібермес бұрын барлық құпия ақпаратты жойыңыз.

collect.sh скриптісін пайдаланып, Linux операциялық жүйесі бар клиенттік құрылғыдан диагностикалық ақпаратты жүктеп алу үшін:

1. collect.sh скриптісін жүктеп алыңыз, ол collect.tar.gz мұрағатына жинақталған.
2. Жүктелген мұрағатты диагностикалау қажет Linux операциялық жүйесі бар клиент құрылғыға көшіріңіз.
3. collect.tar.gz мұрағатын шығару үшін келесі пәрменді орындаңыз:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Скриптіні орындауға құқықтарын көрсету үшін келесі пәрменді орындаңыз:

   ```
   # chmod +x collect.sh
   ```

5. collect.sh скриптісін әкімші құқықтары бар есептік жазба арқылы іске қосыңыз:

   ```
   # ./collect.sh
   ```

Диагностикалық ақпараты бар файл /tmp/$HOST_NAME-collect.tar.gz қалтасында жасалады және сақталады.

Файлдарды Карантинге және Сақтық көшірмелеу жүктеу және одан жою

Бұл бөлімде, файлдарды Карантин мен Сақтық көшірмелеу Kaspersky Security Center Web Console веб-консоліне жүктеу және одан жою тәсілі туралы ақпарат келтірілген.

Файлдарды Карантинге және Сақтық көшірмелеуге жүктеу

Келесі екі шарттың бірі орындалса ғана, файлдарды Карантин мен Сақтық көшірмелеуден жүктеп алуға болады: құрылғының сипаттарында **Басқару серверімен байланысты үзбеу** параметрі қосулы болса немесе қосылым шлюзі қолданылса. Әйтпесе, жүктеп алу мүмкін емес.

Файлдың көшірмесін карантиннен немесе Сақтық көшірмелеу қатты дискіге сақтау үшін:

1. Келесі әрекеттердің бірін орындаңыз:

   - Карантиндегі файлдың көшірмесін сақтағыңыз келсе, басты мәзірде **Операциялар** → **Қоймалар** → **Карантин** бөліміне өтіңіз.

   - Сақтық көшірмелеудегі файлдың көшірмесін сақтағыңыз келсе, басты мәзірде **Операциялар** → **Қоймалар** → **Сақтық көшірмелеу** бөліміне өтіңіз.

2. Ашылған терезеде жүктегіңіз келетін файлды таңдап, **Жүктеп алу** түймесін басыңыз.

   Жүктеу басталады. Клиент құрылғысында Карантинге салынған файл көшірмесі көрсетілген қалтаға сақталады.

Kaspersky Security Center Web Console интерфейсінің тілін өзгерту

Kaspersky Security Center Web Console интерфейсінің тілін таңдауға болады.

Интерфейс тілін өзгерту үшін:

1. Қолданбаның негізгі терезесінде **Параметрлер** → **Тіл** бөліміне өтіңіз.

2. Қолдау көрсетілетін локализация тілдерінің бірін таңдаңыз.

API анықтамалық нұсқаулығы

Kaspersky Security Center OpenAPI анықтамалық нұсқаулығы келесі мәселелерді шешуге арналған:

- Автоматтандыру және конфигурациялау. Басқару консолі арқылы қолмен орындағыңыз келмейтін тапсырмаларды автоматтандыруға болады. Сондай-ақ, Басқару консолінде әлі қолдау көрсетілмейтін өзіндік сценарийлерді де қолдана аласыз. Мысалы, әкімші ретінде сіз Kaspersky Security Center OpenAPI интерфейсін басқару топтарының құрылымын әзірлеуді жеңілдететін және оны өзекті күйде ұстайтын сценарийлерді құру және іске қосу үшін пайдалана аласыз.

- Пайдаланушы әзірлемесі. Мысалы, сіз шектеулі әрекеттер жиынтығына мүмкіндік беретін клиенттеріңіз үшін Microsoft Management Console (MMC) негізінде балама Басқару консолін жасай аласыз.

OpenAPI анықтамалық нұсқаулығынан қажетті ақпаратты табу үшін экранның оң жағындағы іздеу өрісін пайдалануға болады.

OpenAPI анықтамалық нұсқаулығы

Сценарийлер мысалы

OpenAPI анықтамалық нұсқаулығында төмендегі кестеде көрсетілген Python сценарийлерінің мысалдары бар. Мысалдар OpenAPI әдістерін қалай шақыруға болатынын және желіні қорғаудың әртүрлі тапсырмаларын автоматты түрде орындауға болатынын көрсетеді, мысалы, "негізгі/қосалқы" иерархияны құру, Kaspersky Security Center бағдарламасында тапсырмаларды іске қосу немесе тарату нүктелерін тағайындау. Сіз мысалдарды сол күйінде басқара аласыз немесе олардың негізінде жеке сценарийлер жасай аласыз.

OpenAPI әдістерін шақыру және сценарийлерді іске қосу үшін:

1. KlAkOAPI.tar.gz мұрағатын жүктеп алыңыз. Бұл мұрағатта KlAkOAPI пакеті және мысалдар бар (оларды мұрағаттан немесе OpenAPI анықтамалық нұсқаулығынан көшіріп алуға болады). KlAkOAPI.tar.gz мұрағаты Kaspersky Security Center орнату қалтасында болады.

2. Басқару сервері орнатылған құрылғыда KlAkOAPI.tar.gz мұрағатынан KlAkOAPI пакетін орнатыңыз.

   OpenAPI әдістерін шақыру, мысалдар мен сценарийлеріңізді іске қосу тек Басқару сервері мен KlAkOAPI пакеті орнатылған құрылғыларда ғана жүзеге асырылуы мүмкін.

Kaspersky Security Center OpenAPI пайдаланушы сценарийлері мен әдістері мысалдарын салыстыру

Мысалы	Мысалдың мақсаты	Сценарий
KlAkParams оқиғалар журналы	`KlAkParams` деректер құрылымын пайдалану арқылы деректерді шығарып, өңдей аласыз. Мысалда осы деректер құрылымымен қалай жұмыс істеу керектігі көрсетілген. Шығару мысалын әртүрлі тәсілдермен көрсетуге болады. HTTP әдісін жіберу үшін деректерді алуға немесе оларды кодта пайдалануға болады.	Бақылау және есеп беру
"Негізгі/қосалқы" иерархияны құру және жою	Сіз қосалқы Басқару серверін қосып, осылайша "Басты сервер - қосалқы сервер" иерархиялық қатынасын орната аласыз. Немесе қосалқы Басқару серверін иерархиядан шығаруға болады.	• Басқару серверлерінің иерархиясын жасау: қосалқы Басқару серверін қосу • Басқару серверлерінің иерархиясын жою

Мысалы	Мысалдың мақсаты	Сценарий
Active Directory бөлімшесі негізінде құрылымы бар топ иерархиясын жасаңыз.	Сіз Active Directory бөлімшесіне сауалнама жүргізіп, анықталған құрылғылар топтарының иерархиясын құра аласыз.	Басқару топтарын жасау
Active Directory кэштелген бөлімшесі негізінде құрылымы бар топ иерархиясын жасаңыз.	Сіз Active Directory бөлімшесінің бұрын жүргізілген сауалнамасы негізінде басқарылатын құрылғылар топтарының иерархиясын құра аласыз. Егер соңғы сауалнамадан кейін Active Directory бөлімшесінде жаңа құрылғылар пайда болса, олар топқа қосылады, өйткені олар сақталған сауалнама нәтижелерінде жоқ.	Басқару топтарын жасау
Желі тізімінің файлдарын көрсетілген құрылғыға қосылым шлюзі арқылы жүктеңіз	Сіз өзіңіздің құрылғыңыздағы Желілік агентке қосылым шлюзі арқылы қосыла аласыз, содан кейін желілер тізімі бар файлды компьютерге жүктей аласыз.	Тарату нүктелері мен қосылым шлюздерін конфигурациялау
Негізгі Басқару сервері қоймасында сақталған лицензиялық кілтті қосалқы Басқару серверлеріне орнатыңыз	Сіз негізгі Басқару серверіне қосыла аласыз, одан қажетті лицензиялық кілтті жүктей аласыз және сол кілтті иерархияға кіретін барлық қосалқы Басқару серверлеріне жібере аласыз.	Басқарылатын бағдарламаларды лицензиялау
Пайдаланушының тиімді құқықтары туралы есепті жасаңыз	Сіз әртүрлі есептерді жасай аласыз. Мысалы, сіз осы мысалды қолдана отырып, тиімді пайдаланушы құқықтары туралы есеп жасай аласыз. Бұл есепте пайдаланушының тобы мен рөліне байланысты құқықтары туралы ақпарат берілген. Есепті HTML, PDF немесе Excel пішімінде жүктеуге болады.	Есепті жасау және қарау
Құрылғы үшін тапсырманы іске қосу.	Сіз өзіңіздің құрылғыңыздағы Желілік агентке қосылым шлюзі арқылы қосыла аласыз, содан кейін қажетті тапсырманы іске қоса аласыз.	Тапсырманы қолмен іске қосу
Active Directory сайты мен қызметтері негізінде IP ішкі желілерін жасау	Сіз қолданатын Active Directory бөлімшесі негізінде IP ішкі желісін құра аласыз. Мысалда көрсетілген IP мекенжайлары ауқымы бойынша сауалнама жүргізіліп, жаңа ішкі желімен қайшылықты болдырмау үшін анықталған ішкі желілер жойылады. Сондықтан, ішкі желілерді сақтау маңызды желіде мұндай мысалды іске қоспаңыз. Сауалнамадан кейін, мысал коды Active Directory бөлімшесіне жүгінеді, ондағы әрбір құрылғыны тексереді және IP ішкі желісін жасайды. Ол үшін, мысалда барлық құрылғылардың бүркеніштері мен IP мекенжайлары қолданылады.	Желі қорғанысын конфигурациялау
Топтағы құрылғылар үшін тарату нүктелерін тіркеу	Сіз басқарылатын құрылғыларды тарату нүктелеріне тағайындай аласыз (бұрын "жаңарту агенттері" деп аталған).	Kaspersky дерекқорлары мен бағдарламаларын жаңарту
Барлық топтарды атап көрсету	Басқару топтарымен әртүрлі әрекеттерді орындауға болады. Мысалда келесілерді қалай орындау керектігі көрсетілген: • "Басқарылатын құрылғылар" түбірлік тобы идентификаторын алу. • Топ иерархиясы бойынша жылжытуға болады. • Топтардың толық иерархиясын олардың атаулары мен ұяшықтарымен бірге алыңыз.	Басқару серверін конфигурациялау
Тапсырмаларды тізімдеу, тапсырмалар статистикасын сұрау және тапсырмаларды іске қосу	Сіз келесі ақпаратты оқып таныса аласыз: • Тапсырманы орындау тарихы. • Тапсырманың ағымдағы күйі. • Әртүрлі күйлердегі тапсырмалар саны. Сондай-ақ, сіз тапсырманы іске қоса аласыз. Әдепкі бойынша, мысал статистиканы шығарғаннан кейін тапсырманы іске қосады.	Тапсырманы орындау барысын бақылау
Тапсырманы жасау және іске қосу	Сіз тапсырманы жасай аласыз. Мысалда келесі тапсырма параметрлерін көрсетіңіз: • Түрі • Іске қосу тәсілі • Атауы • Тапсырма қолданылатын құрылғы тобы Әдепкі бойынша, мысалда "Хабарды көрсету" түріндегі тапсырма жасалады. Бұл тапсырманы барлық басқарылатын Басқару сервері құрылғылары үшін іске қосуға болады. Қажет болса, сіз өзіңіздің тапсырма параметрлерін көрсете аласыз.	Тапсырманы жасау

Мысалы	Мысалдың мақсаты	Сценарий
Лицензиялық кілттерді атап көрсету	Басқару серверінің басқарылатын құрылғыларында орнатылған Kaspersky бағдарламаларына арналған барлық белсенді лицензиялық кілттердің тізімін алуға болады. Тізімде әрбір лицензиялық кілт туралы егжей-тегжейлі мәлімет, мысалы атауы, түрі немесе жарамдылық мерзімі келтірілген.	Қолданылатын лицензиялық кілттер туралы ақпаратты қарап шығу
Ішкі пайдаланушыны жасау және іздеу	Есепті жазбаны одан әрі жұмыс істеу үшін жасай аласыз.	Басқару серверін іске қосу үшін есептік жазбаны таңдау
Пайдаланушы санатын жасау	Сіз қажетті параметрлері бар бағдарламалар санатын жасай аласыз.	Қолмен толықтырылатын бағдарламалар санатын жасау
Пайдаланушыларды SrvView арқылы атап көрсету	Сіз Басқару серверінен егжей-тегжейлі ақпаратты сұрау үшін SrvView класын қолдана аласыз. Мысалы, осы мысалды қолдана отырып, пайдаланушылар тізімін ала аласыз.	Пайдаланушы есептік жазбаларын басқару

OpenAPI арқылы Kaspersky Security Center бағдарламасымен өзара әрекеттесетін бағдарламалар

Кейбір бағдарламалар OpenAPI арқылы Kaspersky Security Center бағдарламасымен өзара әрекеттеседі. Мұндай қолданбаларға, мысалы, Kaspersky мақсатты шабуылдардан қорғау платформасы немесе Kaspersky Security for Virtualization кіреді. Бұл сонымен қатар OpenAPI негізінде сіз әзірлейтін арнаулы клиенттік қолданба болуы мүмкін.

OpenAPI арқылы Kaspersky Security Center бағдарламасымен өзара әрекеттесетін бағдарламалар Басқару серверіне қосылады. Басқару серверіне қосылу үшін рұқсат етілген IP мекенжайларының тізімін конфигурациялаған болсаңыз, Kaspersky Security Center OpenAPI пайдаланатын бағдарламалар орнатылған құрылғылардың IP мекенжайларын қосыңыз. Сіз қолданатын бағдарлама OpenAPI-мен жұмыс істейтінін білу үшін осы бағдарламаның анықтамасын қараңыз.

Провайдерлер үшін үздік тәжірибелер

Бұл анықтамада сіз Kaspersky Security Center конфигурациялау және пайдалану туралы ақпаратты таба аласыз.

Құжатта бағдарламаны орналастыру, конфигурациялау және пайдалану бойынша ұсыныстар, сондай-ақ бағдарлама жұмыс істеген кезде туындайтын типтік мәселелерді шешу тәсілдері бар.

Kaspersky Security Center орналастыруды жоспарлау

Kaspersky Security Center құрамдастарын ұйымның желісінде орналастыруды жоспарлағанда келесі факторларды ескеру қажет:

- Құрылғылардың жалпы санын
- MSP клиенттерінің саны

Бір Басқару сервері 100 000-нан аспайтын құрылғыларға қызмет көрсете алады. Егер ұйымның желісіндегі құрылғылардың жалпы саны 100 000-нан асса, орталықтандырылған басқаруды жеңілдету үшін иерархияға біріктірілген бірнеше Басқару серверлерін MSP жағына орналастыру керек.

Бір басқару серверінде 500-ге дейін виртуалды сервер жасауға болады, сондықтан әрбір 500 MSP клиентіне бөлек басқару сервері қажет.

Орналастыруды жоспарлау кезеңінде Басқару серверіне X.509 арнайы сертификатын белгілеу қажеттілігін ескеру қажет. Басқару серверіне X.509 арнайы сертификатын белгілеу келесі жағдайларда орынды болуы мүмкін (толық емес тізім):

- SSL termination proxy арқылы SSL трафигін инспекциялау үшін;
- сертификат өрістерінің қажетті мәндерін белгілеу үшін;
- сертификаттың қажетті криптографиялық беріктігін қамтамасыз ету үшін.

Басқару серверіне интернеттен қатынасуды ұсыну

Клиенттің желісінде орналастырылған құрылғылар Басқару серверіне интернет арқылы жүгіне алуы үшін, Басқару серверінің келесі порттарын қолжетімді ету керек:

- 13000 TCP – Басқару серверінің TLS порты, осы портқа клиент желісінде орналастырылған Желілік агенттер қосылады
- 8061 TCP – автономды пакеттерді Басқару консолінің құралдарымен жариялау үшін қолданылатын HTTPS порты

- 8060 TCP – автономды пакеттерді Басқару консолінің құралдарымен жариялау үшін қолданылатын HTTPS порты

- 13292 TCP – бұл TLS порты тек ұялы құрылғыларды басқару қажет болғанда ғана керек

Клиенттерге өз желіңізді Kaspersky Security Center Web Console арқылы басқару бойынша базалық мүмкіндіктерді ұсыну қажет болса, Kaspersky Security Center Web Console веб-консолінің 8080 TCP портын (HTTPS-портты) ашу керек.

Kaspersky Security Center типтік конфигурациясы

MSP серверлерінде бір немесе бірнеше Басқару сервері орналасқан. Серверлер саны қолжетімді аппараттық жасақтаманың болуына байланысты, сондай-ақ қызмет көрсетілетін MSP клиенттерінің санына немесе басқарылатын құрылғылардың жалпы санына байланысты таңдалуы мүмкін.

Бір Басқару сервері 100 000-ға дейінгі құрылғыларға қызмет көрсете алады. Таяу болашақта басқарылатын құрылғылардың санын көбейту мүмкіндігін ескеру қажет: бір Басқару серверіне біршама аз құрылғыларды қосу қажет болуы мүмкін.

Бір басқару серверінде 500-ге дейін виртуалды сервер жасауға болады, сондықтан әрбір 500 MSP клиентіне бөлек басқару сервері қажет.

Егер бірнеше Сервер болса, оларды иерархияға біріктіру ұсынылады. Басқару серверлерінің иерархиясының болуы саясат пен тапсырмалардың қайталануын болдырмауға, барлық басқарылатын құрылғылардың көпшілігімен олардың барлығы бір Басқару серверімен басқарылатындай жұмыс істеуге: құрылғыларды іздеуге, құрылғы таңдауларын жасауға, есептер жасауға мүмкіндік береді.

MSP клиентіне сәйкес келетін әрбір виртуалды серверде бір немесе бірнеше тарату нүктесін тағайындау керек. MSP клиенттері мен Басқару сервері арасындағы байланыс интернет арқылы жүзеге асырылатындықтан, тарату нүктелері үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасын, тарату нүктелері жаңартуларды Басқару серверінен емес, тікелей Kaspersky серверлерінен жүктеп алатындай етіп жасаған жөн.

Егер MSP клиентінің желісінде құрылғылардың бір бөлігі интернетке тікелей қатынаса алмаса, онда тарату нүктелерін қосылым шлюзі режиміне ауыстыру керек. Бұл жағдайда, MSP клиентінің желісіндегі құрылғылардағы Желілік агенттер Басқару серверіне тікелей емес, шлюз арқылы қосылады (синхрондау мақсатында).

Басқару сервері MSP клиентінің желісінде сауалнама өткізе алмайтындықтан, бұл функцияны орындау міндетін тарату нүктелерінің біріне жүктеген жөн.

Басқару сервері MSP клиентінің желісінде NAT артында орналасқан басқарылатын құрылғыларға 15000 UDP портына хабарландыру жібере алмайды. Бұл мәселені шешу үшін, тарату нүктелері болып табылатын және қосылымдар шлюзі режимінде жұмыс істейтін құрылғылардың сипаттарында Басқару серверімен тұрақты қосылу режимін қосқан жөн (**Басқару серверімен байланысты үзбеу** жалаушасы). Егер тарату нүктелерінің жалпы саны 300-ден аспаса, тұрақты қосылу режимі қолжетімді болады.

Тарату нүктелері туралы

Желілік агенті орнатылған құрылғыны тарату нүктесі ретінде пайдалануға болады. Бұл режимде, Желілік агент келесі функцияларды орындай алады:

- Файлдарды клиент құрылғыларына тасымалдау, соның ішінде:
  - Kaspersky дерекқорлары мен бағдарламалық жасақтама модульдері

    Жаңартуларды басқару серверінен немесе Kaspersky серверлерінен шығарып алуға болады. Соңғы жағдайда, тарату нүктесі болып табылатын құрылғы үшін *Жаңартуларды тарату орындарының қоймаларына жүктеп алу* тапсырмасы жасалуы тиіс.
  - Үшінші тарап бағдарламалық жасақтамасының жаңартулары
  - Орнату пакеттері
  - Басқару серверін WSUS сервері ретінде пайдаланған кездегі Windows жаңартулары
- Бағдарламалық жасақтаманы басқа құрылғыларға орнату, соның ішінде құрылғыларда Желілік агенттерді бастапқы орналастыруды орындау.
- Жаңа құрылғыларды анықтау және бұрыннан белгілі құрылғылар туралы ақпаратты жаңарту мақсатымен желіні сұрастыру. Тарату нүктесі Басқару серверімен бірдей құрылғыларды табу әдістерін қолдануы мүмкін.

Тарату нүктелерін ұйымның желісіне орналастыру келесі мақсаттарды көздейді:

- Егер жаңарту көзі Басқару сервері болса, Басқару серверіне түсетін жүктемені азайтыңыз.
- Интернет-трафикті оңтайландыру, өйткені бұл жағдайда MSP клиентінің желісіндегі әрбір құрылғыға жаңартулар алу үшін Kaspersky серверлеріне немесе Басқару серверіне жүгінудің қажеті жоқ.
- MSP клиенті желісінің NAT артындағы (Басқару серверіне қатысты) құрылғыларға Басқару серверіне қатынасу мүмкіндігін ұсыну Басқару серверіне келесі әрекеттерді орындауға мүмкіндік береді:
  - IPv4 немесе IPv6 желілеріндегі UDP арқылы құрылғыларға хабарландырулар жіберу
  - IPv4 немесе IPv6 желісінде сауалнама өткізу
  - Бастапқы орналастыруды орындау
  - push-сервер ретінде қолдану

Тарату нүктесі басқару тобына тағайындалады. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымы осы басқару тобындағы және оның барлық ішкі топтарындағы құрылғылар болады. Бұл арада, тарату нүктесі ретінде әрекет ететін құрылғы, өзі тағайындалған басқару тобына тиесілі болмауы керек.

Сіз тарату нүктесін қосылым шлюзі етіп жасай аласыз. Бұл жағдайда, тарату нүктесінің әрекет ету ауқымындағы құрылғылар Басқару серверіне тікелей емес, шлюз арқылы қосылады. Бұл режим Желілік агенті мен Басқару сервері бар құрылғылар арасында тікелей байланыс орнату мүмкін болмайтын сценарийлерде пайдалы.

Тарату нүктелері рөлін атқаратын құрылғылар рұқсатсыз қол жеткізудің кез келген түрінен, соның ішінде физикалық тұрғыдан қорғалуы тиіс.

Басқару серверлерінің иерархиясы

MSP-де бірден артық Басқару сервері болуы мүмкін. Бірнеше шашыраңқы Серверлерді басқару ыңғайсыз, сондықтан оларды иерархияға біріктірген жөн. Екі Басқару сервері арасындағы "негізгі – қосалқы" өзара іс-қимылы келесі мүмкіндіктер ұсынады:

- Қосалқы Сервер басты Серверден саясаттар мен тапсырмаларды иеленеді, параметрлердің қайталануы жойылады.
- Басқару сервердегі құрылғыны таңдауларға қосалқы Басқару серверлердегі құрылғылар қосылуы мүмкін.
- Басты Басқару сервердегі есептерге қосалқы Басқару серверлердегі деректер (соның ішінде егжей-тегжейлі) қосылуы мүмкін.

Негізгі Басқару сервері жоғарыда берілген параметрлер аясында деректерді виртуалды емес, тәуелді басқару серверлерінен ғана алады. Бұл шектеулер негізгі басқару серверімен бір дерекқорды пайдаланатын виртуалды басқару серверлеріне қолданылмайды.

Виртуалды Басқару серверлері

Физикалық Басқару серверінің шеңберінде бірнеше виртуалды Басқару серверлерін құруға болады, олардың көпшілігі қосалқы Серверлерге ұқсас. Қатынасуды бақылау тізіміне (ACL) негізделген қатынасуды бөлу моделімен салыстырғанда, виртуалды Серверлер моделі анағұрлым функционалды болып келеді және оқшаулаудың үлкен дәрежесін ұсынады. Саясат пен тапсырма құрылғыларына тағайындауға арналған басқару топтарының құрылымынан басқа, әрбір виртуалды Басқару серверінің өзіндік тағайындалмаған құрылғылар тобы, өзіндік есептер жиынтығы, құрылғыларды таңдау және оқиғалар, орнату пакеттері, жылжыту ережелері және т.б. бар. MSP клиенттерін максималды түрде өзара оқшаулау мақсатында, белгілі бір тапсырмалар үшін қолданылатын виртуалды Басқару серверлерін таңдау ұсынылады. Сонымен қатар, әрбір MSP клиенті үшін виртуалды Серверді құру клиенттерге Kaspersky Security Center Web Console арқылы өз желісін басқару бойынша негізгі мүмкіндіктерді ұсынуға мүмкіндік береді.

Виртуалды Серверлер көбінесе қосалқы Басқару серверлеріне ұқсас болып келеді, алайда олардың келесі айырмашылықтары бар:

- виртуалды Серверде көптеген жаһандық параметрлер мен өзіндік TCP порттары жоқ;
- виртуалды Серверде қосалқы Серверлер болуы мүмкін емес;
- виртуалды Серверде өзінің виртуалды Серверлері болуы мүмкін емес;
- физикалық Басқару серверінде, оның барлық виртуалды Серверлерінің басқарылатын құрылғыларынан (карантин элементтері, бағдарламалар тізімдемесі және т.б.) құрылғылар, топтар, оқиғалар мен нысандар көрінеді;
- виртуалды Сервер желіні тек оған қосылған тарату нүктелері арқылы сканерлей алады.

Kaspersky Endpoint Security for Android орнатылған ұялы құрылғыларын басқару

Kaspersky Endpoint Security for Android орнатылған (бұдан әрі KES құрылғылары) ұялы құрылғыларды басқару Басқару сервері арқылы жүргізіледі. Kaspersky Security Center KES құрылғыларды басқарудың келесі мүмкіндіктеріне қолдау көрсетеді:

- Ұялы құрылғылармен клиент құрылғысына ұқсас жұмыс істеу:
  - Басқару топтарына мүшелік
  - Мониторинг, мысалы күйлерді, оқиғаларды және есептерді қарау
  - Жергілікті параметрлерді өзгерту және Android үшін Kaspersky Endpoint Security қолданбасына арналған саясаттарды тағайындау
- Пәрмендерді орталықтандырылған жіберу
- Ұялы қолданбалар пакетін қашықтан орнату

Басқару сервері KES құрылғыларды TLS протоколы, 13292 TCP-порты арқылы басқарады.

Орналастыру және бастапқы конфигурациялау

Kaspersky Security Center бағдарламасы таратылған бағдарлама болып саналады. Kaspersky Security Center құрамына келесі бағдарламалар кіреді:

- Басқару сервері – ұйымның құрылғыларын басқару және деректерді ДҚБЖ-де сақтау үшін жауапты орталық құрамдас.
- Басқару консолі – әкімшінің негізгі құралы. Басқару консолі Басқару серверімен бірге жеткізіледі, бірақ әкімшінің бір немесе бірнеше құрылғысына бөлек орнатылуы мүмкін.
- Kaspersky Security Center Web Console – қарапайым операцияларды орындауға арналған Басқару серверінің веб-интерфейсі. Бұл құрамдасты аппараттық және бағдарламалық жасақтамаға қойылатын талаптарға сай келетін кез келген құрылғыға орнатуға болады.
- Желілік агент – құрылғыда орнатылған қауіпсіздік бағдарламасын басқару, сондай-ақ құрылғы туралы ақпаратты алу үшін қолданылады. Желілік агенттер ұйымның құрылғыларына орнатылады.

Kaspersky Security Center бағдарламасын ұйымның желісінде орналастыру келесі тәсілдермен жүзеге асырылады:

- Басқару серверін орнату;
- Kaspersky Security Center Web Console орнату;
- Басқару консолін әкімшінің құрылғысына орнату;
- Желілік агент пен қауіпсіздік бағдарламаларын ұйымның құрылғыларына орнату.

Басқару серверін орнату бойынша ұсыныстар

Осы бөлімде Басқару серверін орнатуға қатысты ұсынымдар бар. Бөлімде клиент құрылғыларында Желілік агентті орналастыруға арналған Басқару серверін қамтитын құрылғыда ортақ қатынасы бар қалталарды қолдану сценарийлері де бар.

Істен шығуға төзімді кластерде Басқару серверінің қызметтеріне арналған есептік жазбалар жасау

Әдепкі бойынша инсталлятор Басқару серверінің қызметтері үшін ерекше артықшылығы жоқ есептік жазбаларды өз бетінше жасайды. Мұндай жүріс-тұрыс Басқару серверін кәдімгі құрылғыға орнату үшін анағұрлым қолайлы.

Алайда Басқару серверін істен шығуға төзімді кластерге орнатқан кезде басқаша жасау керек:

1. Басқару серверінің қызметтері үшін ерекше артықшылығы жоқ домендік есептік жазбалар жасау және оларды KLAdmins жаһандық домендік қауіпсіздік тобының мүшелеріне айналдыру.

2. Басқару серверінің инсталляторында қызметтер үшін жасалған домендік есептік жазбаларды белгілеу.

ДҚБЖ таңдау

Басқару сервері пайдаланатын ДҚБЖ таңдау кезінде Басқару сервері қызмет көрсететін құрылғылардың санын басшылыққа алу керек.

Төмендегі кестеде ДҚБЖ рұқсат етілген нұсқалары және оларды ұсынымдары мен қолдану шектеулері аталған.

ДҚБЖ ұсынымдар және шектеулер

ДҚБЖ	Ұсынымдар және шектеулер
SQL Server Express Edition 2016 және одан жоғары	10 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Дерекқордың толып кетуіне жол бермеу үшін оқиғалар қоймасындағы оқиғалардың ең көп санын шектей аласыз. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу. SQL Server Express Edition ДҚБЖ Басқару серверімен және қандай да бір басқа бағдарламамен бірге қолдануға болмайды. Microsoft SQL Express дерекқорына **Windows Update жаңартуларын синхрондау** тапсырмасы үшін қолдау көрсетілмейді.
Express, 2016 және одан жоғары нұсқасынан ерекшеленетін жергілікті SQL Server Edition	Шектеулер жоқ.
Express, 2016 және одан жоғары нұсқалардан ерекшенелетін қашықтағы SQL Server Edition	Егер екі құрылғы бір Windows доменінде болса ғана рұқсат етіледі; егер домендер әртүрлі болса, онда олардың арасында екі жақты сенім қатынасы орнатылуы тиіс.

ДҚБЖ	Ұсынымдар және шектеулер
Жергілікті немесе қашықтағы MySQL 5.5, 5.6 немесе 5.7 (MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 және 5.5.5 нұсқаларына қолдау көрсетілмейді)	10 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.
Жергілікті немесе қашықтағы MySQL 8.0.20 немесе одан жоғары	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.
Жергілікті немесе қашықтағы MariaDB нұсқасы (қолдау көрсетілетін нұсқаларды қараңыз)	20 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.
PostgreSQL, Postgres Pro (қолдау көрсетілетін нұсқаларды қараңыз)	50 000-нан аз құрылғылар үшін бір Басқару серверін пайдалануды жоспарласаңыз, осы ДҚБЖ жүйелерінің бірін пайдаланыңыз. Бағдарламалық жасақтаманы түгендеу тапсырмасы тапсырмасын өшіру және Басқару серверінің бағдарламаларды іске қосу туралы хабарландыруларын өшіру (Kaspersky Endpoint Security саясатының параметрлерінде) ұсынылады. Қосымша ақпарат алу үшін қараңыз: Дерекқордағы орынды есептеу.

Егер сіз MSSQL 2019 нұсқасын таңдасаңыз, CU12 немесе одан кейінгі жинақталған патчын пайдалануыңыз керек. Бұл сізге орын алуы мүмкін қателер мен жүйенің шамадан тыс жүктелуін болдырмауға мүмкіндік береді.

PostgreSQL, MariaDB немесе MySQL ДҚБЖ пайдалансаңыз, **Оқиғалар** қойындысы таңдалған клиент құрылғысы үшін оқиғалардың толық тізімін көрсетпеуі мүмкін. Бұл, ДҚБЖ оқиғалардың өте көп санын сақтаған кезде орын алады. Келесі әрекеттердің бірін орындау арқылы көрсетілетін оқиғалар санын көбейтуге болады:

- Керек емес оқиғаларды жою.
- Керек емес оқиғаларды сақтау мерзімін қысқарту.

Құрылғы үшін Басқару серверінде тіркелген оқиғалардың толық тізімін көру үшін Есептерді пайдаланыңыз.

Басқару серверінің мекенжайын көрсету

Басқару серверін орнатқан кезде, Басқару серверінің сыртқы мекенжайын белгілеу қажет. Бұл мекенжай, әдепкі бойынша Желілік агенттің орнату пакеттерін жасау кезінде қолданылады. Алдағыда, Басқару серверінің мекенжайын Басқару консолі арқылы өзгертуге болады, бірақ бұл арада ол қазірдің өзінде жасалған Желілік агенттің орнату пакеттерінде автоматты түрде өзгермейді.

Ұйым-клиент желісінде қорғанысты конфигурациялау

Басқару серверінің инсталляциясын аяқталғаннан кейін шебердің көмегімен бастапқы конфигурациялауды орындауды ұсынатын Басқару консолі іске қосылады. Бағдарламаны жылдам іске қосу шеберінің жұмысы уақытында түпкі басқару тобында келесі саясаттар мен тапсырмалар жасалады:

- Kaspersky Endpoint Security саясаты
- Kaspersky Endpoint Security жаңарту топтық тапсырмасы
- Kaspersky Endpoint Security құрылғысын тексерудің топтық тапсырмасы
- Желілік агент саясаты
- Осалдықтарды іздеу тапсырмасы (Желілік агенттің тапсырмасы)
- Жаңартуларды орнату және осалдықты түзету тапсырмасы (Желілік агенттің тапсырмасы)

Саясаттар мен тапсырмалар осы ұйым үшін оңтайлы емес немесе тіпті жарамсыз болуы мүмкін әдепкі бойынша параметрлермен жасалады. Сондықтан жасалған нысандардың сипаттарын қарастырып, қажет болса, өзгерістерді қолмен енгізу керек.

Осы бөлім Басқару серверінің саясаттарын, тапсырмаларын және басқа параметрлерін қолмен конфигурациялау туралы ақпаратты, сондай-ақ тарату нүктелері, басқару тобының құрылымын құру, тапсырмалардың иерархиясы мен басқа конфигурациялар туралы ақпаратты қамтиды.

Kaspersky Endpoint Security саясатын қолмен конфигурациялау

Осы бөлім Бағдарламаны жылдам іске қосу шебері жасайтын Kaspersky Endpoint Security саясатының параметрлерін конфигурациялау бойынша ұсынымдарды қамтиды. Саясат сипаттары терезесінде конфигурациялауды орындауға болады.

Параметрді өңдеген кезде, оның мәнін жұмыс станциясында пайдалану үшін тиісті параметрдің үстіңгі жағындағы құлып белгішесін басуыңыз керек.

Кеңейтілген қорғаныс бөлімінде саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Кеңейтілген қорғаныс бөлімінде Kaspersky Endpoint Security for Windows үшін Kaspersky Security Network қолданысын конфигурациялауға болады. Сондай-ақ, Әрекеттерді талдау, Эксплойттан қорғаныс, Хост-компьютерге басып кіруді болдырмау және Зиянды әрекеттерді шегіндіру сияқты Kaspersky Endpoint Security for Windows модульдерін конфигурациялауға болады.

Kaspersky Security Network ішкі бөлімінде **Kaspersky Security Network** опциясын қосуға кеңес беріледі. Бұл параметрді пайдалану желі трафигін қайта таратуға және оңтайландыруға көмектеседі. **Kaspersky Security Network** опциясы өшірілсе, KSN серверлерін тікелей пайдалануды қосуға болады.

Негізгі қорғаныс бөліміндегі саясатты конфигурациялау

Бұл бөлімнің параметрлерінің толық сипаттамасы Kaspersky Endpoint Security for Windows құжаттамасында берілген.

Саясат сипаттары терезесінің **Негізгі қорғаныс** бөлімінде **Желілік экран** және **Файл қауіптерінен қорғаныс** ішкі бөлімдерінде қосымша параметрлерді көрсету ұсынылады.

Желілік экран ішкі бөлімі клиент құрылғыларында қолданбалардың желілік әрекетін бақылауға көмектесетін параметрлерді қамтиды. Клиент құрылғысы келесі күйлердің бірі берілген желіні пайдаланады: жалпыға қолжетімді, жергілікті немесе сенімді. Желі күйіне байланысты Kaspersky Endpoint Security құрылғыдағы желілік белсенділікке рұқсат етуі немесе тыйым салуы мүмкін. Ұйымыңызға жаңа желіні қосқан кезде, оған сәйкес желілік күйді беруіңіз керек. Мысалы, егер ноутбук клиент құрылғысы болса, бұл құрылғы жалпыға қолжетімді немесе сенімді желіні пайдалануы ұсынылады, өйткені ноутбук әрқашан жергілікті желіге қосылған болмайды. **Желілік экран** ішкі бөлімінде ұйымда қолданылатын желілерге күйлерді дұрыс тағайындағаныңызды тексеруге болады.

Желілер тізімін тексеру үшін:

1. Саясат сипаттарында **Негізгі қорғаныс** → **Желілік экран** бөліміне өтіңіз.
2. **Қолжетімді желілер** бөлімінде **Параметрлер** түймесін басыңыз.
3. Ашылған **Желілік экран** терезесінде желілер тізімін көру үшін **Желі** қойындысына өтіңіз.

Файл қауіптерінен қорғаныс ішкі бөлімінде желі дискілерін сканерлеуді өшіруге болады. Желілік дисктерді тексеру желілік дисктерге айтарлықтай жүктемені тудыра алады. Тікелей файл серверлерінде тексеруді жүзеге асырған жөн.

Желілік дискіні тексеруді өшіру үшін:

1. Саясат сипаттарында **Негізгі қорғаныс** → **Файл қауіптерінен қорғаныс** бөліміне өтіңіз.
2. **Қауіпсіздік деңгейі** бөлімінде **Параметрлер** түймесін басыңыз.
3. Ашылған **Файл қауіптерінен қорғаныс** терезесіндегі **Жалпы** қойындысында **Барлық желілік дискілер** құсбелгі ұяшығын тазалаңыз.

Қосымша параметрлер бөліміндегі саясатты конфигурациялау

Бұл бөлім параметрлерінің толық сипаттамасы Kaspersky Endpoint Security құжаттамасында берілген.

Төменде **Жалпы параметрлер** бөліміндегі Kaspersky Endpoint Security саясат сипаттары терезесінде орындау ұсынылатын қосымша конфигурация қадамдары сипатталған.

Қосымша параметрлер бөлімі, есептер және қоймалар ішкі бөлімі

Деректерді басқару серверіне жіберу бөлімінде **Іске қосылатын қолданбалар туралы ақпарат** жалаушасына назар аударыңыз. Бұл жалауша қойылған кезде, басқару сервері дерекқоры ұйымның желісіндегі құрылғылардағы барлық қолданба модульдерінің барлық нұсқалары туралы ақпаратты сақтайды. Көрсетілген ақпарат Kaspersky Security Center дерекқорында (ондаған гигабайт) айтарлықтай көлемді алуы мүмкін. Сондықтан жоғары деңгейлі саясатта әлі де **Іске қосылатын қолданбалар туралы ақпарат** жалаушасы қойылса, оны алу керек.

Қосымша параметрлер бөлімі, интерфейс ішкі бөлімі

Басқару консолі арқылы ұйымыңыздың желісіндегі қорғауды орталықтан басқару қажет болса, жұмыс станцияларында Kaspersky Endpoint Security пайдаланушы интерфейсін көрсетуді өшіру керек (**Пайдаланушымен өзара әрекеттесу** бөліміндегі **Қолданба интерфейсін көрсету** жалаушасын алып тастау арқылы) және құпиясөзбен қорғауды (**Құпиясөзбен қорғау** бөліміндегі **Құпиясөзбен қорғауды қосу** жалаушасын қою арқылы) керек.

Оқиғаларды конфигурациялау бөліміндегі саясатты конфигурациялау

Оқиғаларды конфигурациялау бөлімінде төменде аталған оқиғалардан басқа барлық оқиғаны басқару серверінде сақтауды өшіру керек:

- **Критикалық** қойындысында:
  - *Бағдарламаны автоматты түрде іске қосу өшірілді*
  - *Қатынасуға тыйым салынған*
  - *Бағдарламаны іске қосуға рұқсат берілмеген*
  - *Емдеу мүмкін емес*
  - *Түпкі пайдаланушының лицензиялық келісімі бұзылды*
  - *Шифрлау модулін жүктеу мүмкін болмады*
  - *Екі тапсырманы бір уақытта іске қосу мүмкін емес*
  - *Белсенді қауіп анықталды. Белсенді зақымдауды емдеу процедурасын іске қосу керек*
  - *Желілік шабуыл анықталды*
  - *Барлық компоненттер жаңартылмады*
  - *Белсендіру қатесі*
  - *Ықшам режимді белсендіру қатесі*
  - *Kaspersky Security Center орталығымен өзара әрекеттесу қатесі*
  - *Портативті режимді өшіру қатесі*
  - *Бағдарлама компоненттерінің құрамын өзгерту қатесі*

- *Файлдарды шифрлау/шифрын шешу ережелерін қолдану қатесі*
- *Саясатты қолдану мүмкін емес*
- *Процесс аяқталды*
- *Желілік белсенділікке рұқсат берілмеген*

- **Функционалдық ақау** қойындысында: *Тапсырма параметрлеріндегі қате. Тапсырма параметрлері қолданылмады*
- **Ескерту** қойындысында:
  - *Бағдарламаның өзіндік қорғанысы өшірілді*
  - *Резервті кілті дұрыс емес*
  - *Пайдаланушы шифрлау саясатынан бас тартты*
- **Ақпараттық** қойындысында: *Бағдарламаны сынақ режимде іске қосуға тыйым салынған*

Kaspersky Endpoint Security жаңарту топтық тапсырмасын қолмен конфигурациялау

Басқару сервері жаңарту көзі рөлін атқарса, Kaspersky Endpoint Security үшін ұсынылған оңтайлы жоспарлау опциясы — **Тапсырманы бастау үшін автоматты түрде араластырылған кідірісті пайдалану** құсбелгі ұяшығы таңдалған **Қоймаға жаңа жаңартулар жүктеп алынған уақыт**.

Егер әрбір тарату нүктесі үшін Kaspersky серверлерінен жаңартуларды қоймаға жүктеудің жергілікті тапсырмасы жасалса, онда Kaspersky Endpoint Security жаңартудың топтық тапсырмасы үшін кесте бойынша мезгіл-мезгіл іске қосу оңтайлы және ұсынылатын болып саналады. Бұл жағдайда, автономизация кезеңінің мәні 1 сағат болып орнатылуы керек.

Kaspersky Endpoint Security құрылғысын тексеру топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері құрылғыны тексерудің топтық тапсырмасын жасайды. Әдепкі бойынша тапсырма үшін автоматты рандомизациясы бар **Жұма күндері 19:00-де іске қосу** кестесі таңдалды және **Өткізіп алынған тапсырмаларды іске қосу** жалаушасы алынды.

Демек, егер ұйымның құрылғылары жұма күндері сағат 18:30-да сөндірілсе, онда құрылғыны сканерлеу тапсырмасы ешқашан іске қосылмайды. Ұйымда қабылданған жұмыс регламентіне сүйене отырып осы тапсырманың оңтайлы кестесін конфигурациялау керек.

Осалдықтарды және қажетті жаңартуларды іздеу тапсырмасы кестесін конфигурациялау

Бағдарламаны жылдам іске қосу шебері Желілік агент үшін *Осалдықтарды және қажетті жаңартуларды іздеу* топтық тапсырмасын жасайды. Әдепкі бойынша тапсырма үшін автоматты рандомизациясы бар **Сейсенбі күндері 19:00-де іске қосу** кестесі таңдалды және **Өткізіп алған тапсырмаларды іске қосу** жалаушасы орнатылды.

Егер ұйым жұмысының регламенті осы уақытта құрылғыларды сөндіруді қарастырса, онда *Осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыны қосқаннан кейін (сәрсенбі күні таңертең) іске қосылады. Мұнда жүріс-тұрыс жағымсыз болуы мүмкін, өйткені осалдықтарды іздеу құрылғының процессоры мен диск ішкі жүйесіне жоғары жүктеме түсіруі мүмкін. Ұйымда қабылданған жұмыс регламентіне сүйене отырып, тапсырманың оңтайлы кестесін конфигурациялау керек.

Жаңартуларды орнату және осалдықты түзету топтық тапсырмасын қолмен конфигурациялау

Бағдарламаны жылдам іске қосу шебері Желілік агент үшін жаңартуларды орнату және осалдықтарды іздеу топтық тапсырмасын жасайды. Әдепкі бойынша автоматты түрде рандомизациясы бар күн сайын 1:00-де тапсырманы іске қосу конфигурацияланған, **Өткізіп алынған тапсырмаларды іске қосу** параметрі сөндірілген.

Егер ұйымның жұмыс регламенті құрылғыны түнде сөндіруді қарастырса, онда жаңартуларды орнату тапсырмасы ешқашан іске қосылмайды. Ұйымда қабылданған жұмыс регламентіне сүйеніп, осалдықтарды іздеу тапсырмасының оңтайлы кестесін белгілеу керек. Сонымен қатар, жаңартуларды орнату нәтижесінде құрылғыны қайта іске қосу қажет болуы мүмкін екендігін ескерген жөн.

Басқару топтары құрылымын құру және тарату нүктелерін тағайындау

Kaspersky Security Center-дегі басқару топтарының құрылымы келесі функцияларды орындайды:

- Саясаттардың әрекет ету ауқымын белгілеу.

  Саясат профильдерінің көмегімен құрылғыларда параметрлердің сыртқы жиынтықтарын қолданудың баламалы тәсілі бар. Бұл жағдайда саясаттар ауқымы, мысалы, тегтер, құрылғылардың Active Directory ұйымдық бөлімшесінде орналасқан жерлері және Active Directory қауіпсіздік топтарындағы мүшелік арқылы орнатылады.

- Топтық тапсырмалардың әрекет ету ауқымын белгілеу.

  Басқару топтарының иерархиясына негізделмеген топтық тапсырмалардың әрекет ету ауқымын белгілеу тәсілдемесі бар: құрылғыларды таңдау және арнайы құрылғылар үшін тапсырмаларды қолдану.

- Құрылғыларға, виртуалды және қосалқы Басқару серверлеріне қатынасу құқықтарын белгілеу.

- Тарату нүктелерін тағайындау.

Басқару топтарының құрылымын құру кезінде тарату нүктелерін оңтайлы түрде тағайындау үшін ұйым желісінің топологиясын ескеру қажет. Тарату нүктелерінің оңтайлы таралуы арқасында ұйым желісіндегі желілік трафикті азайтуға мүмкіндік беріледі.

MSP клиентінің ұйымдық құрылымына және желілер топологиясына байланысты, басқару топтары құрылымының келесі типтік конфигурацияларын ажыратуға болады:

- Бір кеңсе
- Көптеген шағын оқшауланған кеңселер

MSP клиентінің типтік конфигурациясы: бір кеңсе

"Бір кеңсе" типтік конфигурациясында барлық құрылғылар ұйымның желісінде орналаса отырып, бір-бірін "көреді". Ұйымның желісі тар арналармен байланысқан бірнеше бөлектенген бөліктен (желіден немесе желі сегменттерінен) құралуы мүмкін.

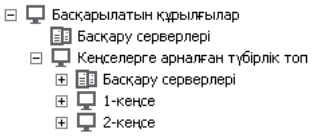
Басқару топтарының құрылымын құрудың келесі тәсілдері болуы мүмкін:

- Желі топологиясын ескере отырып, басқару тобының құрылымын құру. Басқару топтарының құрылымы желінің топологиясын нақты түрде көрсетуге міндетті емес. Желінің бөлектенген бөліктеріне қандай да бір басқару топтарының сай келуі жеткілікті. Тарату нүктелерін автоматты түрде тағайындауды қолдануға немесе тарату нүктелерін қолмен тағайындауға болады.
- Желінің топологиясын білдірмейтін басқару топтарының құрылымын құру. Бұл жағдайда, тарату нүктелерін автоматты түрде тағайындауды өшіру және желінің әрбір бөлектенген бөлігінде түбірлік басқару тобына, мысалы, **Басқарылатын құрылғылар** тобына бір немесе бірнеше құрылғыны тарату нүктелері ретінде тағайындау керек. Барлық тарату нүктелері бір деңгейде болады және бірдей "ұйым желісінің барлық құрылғылары" әрекет ету ауқымына ие болады. Желілік агенттердің әрқайсысы, бағыты ең қысқа болып саналатын тарату нүктесіне қосылатын болады. Тарату нүктесіне апаратын бағытты tracert утилитасының көмегімен анықтауға болады.

MSP клиентінің типтік конфигурациясы: көптеген шағын оқшауланған кеңселер

Бұл типтік конфигурация, бәлкім, басты кеңсемен интернет арқылы байланысқан көптеген шағын қашықтағы кеңселерге сәйкес келеді. Қашықтағы кеңселердің әрқайсысы NAT артында орналасқан, яғни бір қашықтағы кеңседен екіншісіне қосылу мүмкін емес – кеңселер бір-бірінен оқшауланған.

Конфигурация басқару топтарының құрылымында міндетті түрде көрсетілуі керек: қашықтағы кеңселердің әрқайсысы үшін жеке басқару тобын құру керек (төмендегі суреттегі **1-кеңсе**, **2-кеңсе** топтары).



Қашықтағы кеңселер басқару топтарының құрылымында көрсетілген

Кеңсеге сай келетін әрбір басқару тобына бір немесе бірнеше тарату нүктесін тағайындау керек. Дискіде жеткілікті орны бар қашықтағы кеңсе құрылғыларын тарату нүктелері ретінде тағайындау керек. Мысалы, **1-кеңсе** тобында орналастырылған құрылғылар **1-кеңсе** басқару тобына тағайындалған тарату нүктелеріне жүгінетін болады.

Егер кейбір пайдаланушылар ноутбуктері бар кеңселер арасында физикалық түрде жылжытылатын болса, әр қашықтағы кеңседе жоғарыда аталған тарату нүктелеріне тағы екі және немесе одан да көп құрылғыны таңдап, оларды жоғарғы деңгейдегі басқару тобына тарату нүктелері ретінде тағайындау керек (жоғарыдағы суреттегі **Кеңселерге арналған түбірлік топ** тобы).

1-кеңсе басқару тобында болған, бірақ физикалық түрде **2-кеңсе** тобына сәйкес келетін кеңсеге көшірілген ноутбук. Жылжытқаннан кейін, ноутбуктағы Желілік агент **1-кеңсе** тобына тағайындалған тарату нүктелеріне жүгінуге тырысатын болады, бірақ бұл тарату нүктелері қолжетімді болмайды. Сонда Желілік агент **Кеңселерге арналған түбірлік топ** тобына тағайындалған тарату нүктелеріне жүгіне бастайды. Қашықтағы кеңселер бір-бірінен алшақ орналасқандықтан, **Кеңселерге арналған түбірлік топ** басқару тобына тағайындалған барлық тарату нүктелерінен **2-кеңсе** тобына тағайындалған тарату нүктелеріне жүгіну ғана сәтті болады. Яғни, ноутбук өзінің бастапқы кеңсесіне сәйкес келетін басқару тобында бола отырып, қазіргі уақытта физикалық түрде орналасқан кеңсенің тарату нүктесін қолдана беретін болады.

Саясаттар иерархиясы, саясат профильдерін қолдану

Осы бөлім саясаттарды басқару топтарындағы құрылғыларға қолдану ерекшеліктері туралы ақпаратты қамтиды. Осы бөлім саясаттардың профильдері туралы ақпаратты да қамтиды.

Саясаттар иерархиясы

Kaspersky Security Center-де саясаттар көптеген құрылғыларда бірдей параметрлер жинағын белгілеуге арналған. Мысалы, G тобы үшін анықталған P бағдарламасы саясатының әрекет ету ауқымы сипаттарында **Тектік топтан иелену** жалаушасы алынған ішкі топтарды қоспағанда, G басқару тобында және барлық оның ішкі топтарында орналасқан P бағдарламасы орнатылған басқарылатын құрылғылар болып табылады.

Саясат оның ішіндегі параметрлердің жанында "құлыптардың" (🔒) болуымен жергілікті параметрлерден ерекшеленеді. Саясат сипаттарында орнатылған құлып оған сәйкес параметр (немесе параметрлер тобы) біріншіден, тиімді параметрлерді қалыптастырған кезде пайдаланылуы керектігін, екіншіден, төмендегі саясатқа жазылуы керектігін білдіреді.

Құрылғыда әрекет ететін параметрлерді қалыптастыруды келесі түрде көрсетуге болады: саясаттан құлпы орнатылмаған параметрлердің мәндері алынады, кейін олардың үстіне жергілікті параметрлердің мәндері жазылады, кейін алған мәндердің үстіне саясаттан алынған құлпы орнатылған параметрлердің мәндері жазылады.

Бірдей бағдарламаның саясаттары бір-біріне басқару топтарының иерархиясы бойынша әрекет етеді: жоғарыдағы саясаттың орнатылған құлпы бар параметрлері төмендегі саясаттың аттас параметрлерін қайта жазады.

Ерекше саясат түрі бар - автономды пайдаланушыларға арналған саясат. Бұл саясат құрылғы автономды режимге ауысқан кезде құрылғыда күшіне енеді. Автономды пайдаланушыларға арналған саясаттар басқа саясаттарға басқару топтарының иерархиясы бойынша әрекет етпейді.

Саясат профильдері

Тек қана басқару топтарының иерархиясына сүйене отырып құрылғыларға саясаттарды қолдану көптеген жағдайларда ыңғайсыз. Әртүрлі басқару топтары үшін саясаттың бірнеше көшірмелерін жасау және одан әрі осы саясаттардың мазмұнын қолмен синхрондау қажеттілігі туындауы мүмкін.

Осындай мәселелерді болдырмауға көмектесу үшін, Kaspersky Security Center *саясаттар профильдерін* қолдайды. Саясат профилі, саясат параметрлерінің аталған ішкі жиынтығы болып табылады. Параметрлердің осы ішкі жиынтығы құрылғыларға саясатпен бірге таралады және келесі шартты – *профильді белсендіру шартын* орындаған кезде саясатты толықтырады. Профильдер клиент құрылғысында (компьютерде, ұялы құрылғыда) әрекет ететін "негізгі" саясаттан ерекшеленетін параметрлерді ғана қамтиды. Профильді белсендірген кезде, профиль белсендірілгенге дейін құрылғыда әрекет еткен саясат параметрлері өзгереді. Бұл параметрлер профильде көрсетілген мәндерді қабылдайды.

Саясаттардың профильдері қазір келесі шектеулерге ие:

- саясатта ең көбі 100 профиль болуы мүмкін;
- саясаттың профилі басқа профильдерді қамти алмайды;
- саясаттың профилі хабарландыру параметрлерін қамти алмайды.

Профильдің мазмұны

Саясаттың профилі келесі құрамдас бөліктерді қамтиды:

- Атауы. Атаулары бірдей профильдер бір-біріне ортақ ережелері бар басқару топтарының иерархиясы арқылы әсер етеді.
- Саясат параметрлерінің қосалқы жиынтығы. Барлық параметрлері бар саясатқа қарағанда, профильде шынымен керек (құлып орнатылған) параметрлер ғана бар.
- Белсендіру шарты – құрылғы сипаттарының логикалық өрнегі. Профиль профильді белсендіру шарты шынайы болған кезде ғана белсенді (саясатты толықтырады). Қалған жағдайларда профиль белсенді емес және ескерілмейді. Логикалық өрнекте құрылғының келесі сипаттары қатыса алады:
  - автономды режим күйі;
  - желілік орта сипаттары – Желілік агентті қосудың белсенді ережесінің атауы;
  - құрылғыда көрсетілген тегтердің болуы немесе болмауы;
  - Active Directory бөлімшесінде құрылғының орналасқан жері: айқын (құрылғы тікелей көрсетілген бөлімшеде орналасқан) немесе айқын емес (құрылғы кез келген тіркеме деңгейінде көрсетілген бөлімшенің ішінде орналасқан бөлімшеде орналасқан);
  - құрылғының Active Directory қауіпсіздік тобындағы мүшелігі (айқын немесе айқын емес);
  - құрылғы иесінің Active Directory қауіпсіздік тобындағы мүшелігі (айқын немесе айқын емес).
- Профильді сөндіру жалаушасы. Сөндірілген профильдер әрқашан ескерілмейді, оларды белсендіру шарттары шынайылыққа тексерілмейді.
- Профильдің басымдығы. Профильдерді белсендіру шарттары тәуелсіз, сондықтан бір уақытта бірден бірнеше профильдер белсендірілуі мүмкін. Егер белсенді профильдер параметрлердің талассыз жинақтарын қамтыса, онда ешқандай мәселелер туындамайды. Дегенмен екі белсенді профильде бірдей параметрдің әртүрлі мәндері болса, түсініксіздік орын алады. Бұл түсініксіздікке профиль басымдықтары арқылы жол бермеу керек: түсініксіздік айнымалысының мәні басымдығы жоғарырақ профильден (профильдер тізімінде жоғары бағаланған) алынады.

Саясаттар иерархия бойынша бір-біріне әрекет еткен кезде профильдердің жағдайы

Аттас профильдер саясаттарды біріктіру ережелеріне сәйкес біріктіріледі. Жоғарғы саясаттың профильдері төменгі саясаттың профильдерінен басымдырақ. Егер "жоғарғы" саясатта параметрлерді өзгертуге тыйым салынса (құлып батырмасы басылған), "төменгі" саясатта "жоғарғы" саясаттағы профильді белсендіру шарттары пайдаланылады. Егер "жоғарғы" саясатта параметрлерді өзгертуге рұқсат етілсе, онда "төменгі" саясаттағы профильді белсендіру шарттары пайдаланылады.

Саясат профилі белсендіру шартында **Құрылғы офлайн режимде** қамти алғандықтан, профиль одан әрі қолдау көрсетілмейтін автономды пайдаланушылар үшін саясаттардың функционалдығын толығымен ауыстырады.

Автономды пайдаланушыларға арналған саясат профильдерді қамтуы мүмкін, бірақ оның профильдерін белсендіру құрылғы автономды режимге ауыспайынша туындамайды.

Тапсырмалар

Kaspersky Security Center *тапсырмаларды* құру және іске қосу арқылы құрылғыларда орнатылған Kaspersky қауіпсіздік бағдарламаларының жұмысын басқарады. Тапсырмалардың көмегімен бағдарламаларды орнату, іске қосу және тоқтату, файлдарды сканерлеу, бағдарламалардың дерекқорлары мен модульдерін жаңарту, бағдарламалармен басқа әрекеттер орындалады.

Бағдарлама үшін басқару плагині орнатылған жағдайда ғана тапсырма жасай аласыз.

Тапсырмалар Басқару серверінде және құрылғыларда орындалуы мүмкін.

Басқару серверінде орындалатын тапсырмалар:

- Есептерді автоматты түрде жеткізу
- Жаңартуларды Басқару серверінің қоймасына жүктеп алу
- Басқару сервері деректерінің сақтық көшірмесін жасау
- Дерекқорларға қызмет көрсету
- Windows Update жаңартуларын синхрондау
- Эталондық құрылғының операциялық жүйесінің кескінінің орнату пакетін жасау

Құрылғыларда тапсырмалардың келесі түрлері орындалады:

- *Жергілікті тапсырмалар* – нақты құрылғыда орындалатын тапсырмалар.

  Жергілікті тапсырмаларды тек әкімші Басқару консолі арқылы ғана емес, қашықтағы құрылғының пайдаланушысы да өзгерте алады (мысалы, қауіпсіздік бағдарламасының интерфейсінде). Егер жергілікті тапсырманы басқарылатын құрылғыда әкімші де, пайдаланушы да бір уақытта өзгерткен болса, онда әкімші енгізген өзгерістер басым болып күшіне енеді.

- *Топтық тапсырмалар* – бұл аталған топтың барлық құрылғыларында орындалатын тапсырмалар.

  Егер тапсырманың сипаттарында басқаша көрсетілмесе, топтық тапсырма аталған топтың ішкі топтарына да таралады. Топтық тапсырмалар (міндетті емес) осы топқа және ішкі топтарға орналастырылған қосалқы және виртуалды Басқару серверлеріне қосылған құрылғыларда да жұмыс істейді.

- *Глобалдық тапсырмалар* – бұл басқару топтарына кіретіндігіне қарамастан, таңдалған құрылғыларда орындалатын тапсырмалар.

Әр бағдарлама үшін сіз топтық тапсырмалардың, глобалдық тапсырмалардың және жергілікті тапсырмалардың кез келген санын жасай аласыз.

Тапсырма параметрлеріне өзгертулер енгізуге, тапсырмалардың орындалуын бақылауға, тапсырмаларды көшіруге, экспорттауға және импорттауға, сондай-ақ жоюға болады.

Құрылғыдағы тапсырмаларды іске қосу тек осы тапсырмалар жасалған бағдарлама іске қосылған жағдайда ғана орындалады.

Тапсырмаларды орындау нәтижелері Microsoft Windows және Kaspersky Security Center, орталықтандырылған түрде Басқару серверінде де, жергілікті түрде әрбір құрылғыда да оқиғалар журналдарында сақталады.

Тапсырмалар параметрлерінде құпия деректерді пайдаланбаңыз. Мысалы, домен әкімшісінің құпиясөзін көрсетпеуге тырысыңыз.

Құрылғыны жылжыту ережелері

MSP клиентіне сай келетін виртуалды сервердегі басқару топтарында құрылғыларды орналастыру, *құрылғыны жылжыту ережелерінің* көмегімен автоматтандырылғаны жөн. Жылжыту ережесі үш негізгі бөліктен тұрады: атауы, орындау шарттары (құрылғы атрибуттарының логикалық өрнегі) және мақсатты басқару тобы. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда ереже құрылғыны мақсатты басқару тобына көшіреді.

Құрылғыны жылжыту ережелерінің басымдықтары бар. Басқару сервері құрылғының атрибуттарын әрбір ережені орындау шартына сай келу тұрғысынан, ережелер басымдығының азаюы тәртібінде тексереді. Құрылғының атрибуттары ережені орындау шартына сай келсе, онда құрылғы мақсатты топқа көшіріледі және бұл құрылғы үшін ережелерді өңдеу осымен тоқтайды. Егер құрылғының атрибуттары бірден бірнеше ережеге сай келсе, онда құрылғы үлкен басымдыққа ие ереженің мақсатты тобына көшіріледі (ережелер тізімінде жоғары тұр).

Құрылғыны жылжыту ережелері айқын емес түрде жасалуы мүмкін. Мысалы, қашықтан орнату тапсырмасының немесе пакетінің сипаттарында, Желілік агентті орнатқаннан кейін құрылғы кіруі тиісті басқару тобы көрсетілуі мүмкін. Сондай-ақ, жылжыту ережелерін Kaspersky Security Center әкімшісі айқын түрде, жылжыту ережелерінің тізімінде жасай алады. Тізім Басқару консолінде, **Тағайындалмаған құрылғылар** тобының сипаттарында орналасқан.

Жылжыту ережесі, әдепкі бойынша құрылғыларды басқару топтарында бір рет бастапқы орналастыруға арналған. Ереже, **Тағайындалмаған құрылғылар** тобындағы құрылғыларды бір рет қана көшіреді. Егер құрылғы бір рет осы ережемен көшірілген болса, тіпті құрылғыны **Тағайындалмаған құрылғылар** тобына қолмен қайтарған жағдайда да, ереже оны қайтадан көшірмейді. Бұл, жылжыту ережелерін қолданудың ұсынылатын тәсілі.

Басқару топтарында әлдеқашан орналастырылған құрылғыларды жылжытуға болады. Бұл үшін, ереженің сипаттарында **Басқару топтарында орналастырылмаған құрылғыларды ғана жылжыту** жалаушасын алып тастау керек.

Басқару топтарында әлдеқашан орналастырылған құрылғыларға қолданылатын жылжыту ережелерінің болуы, Басқару серверіне түсетін жүктемені едәуір арттырады.

Бір құрылғыда көп рет әрекет ете алатын жылжыту ережесін жасауға болады.

Бір құрылғы топтан топқа көп рет жылжыту, мысалы, құрылғыға арнайы саясатты қолдану, арнайы топтық тапсырманы іске қосу, белгілі бір тарату нүктесінен жаңарту мақсатында басқарылатын құрылғылармен жұмыс істеу тәсілдемесінен аулақ болу қатаң ұсынылады.

Мұндай сценарийлерге қолдау көрсетілмейді, өйткені олар Басқару серверіне және желілік трафикке жүктеу бойынша онша тиімсіз. Сондай-ақ, бұл сценарийлер Kaspersky Security Center жұмыс моделіне қарама-қайшы келеді (әсіресе, қатынасу құқықтары, оқиғалар мен есептер саласында). Басқа шешім іздеу, мысалы, саясат профильдерін, құрылғыларды таңдау үшін тапсырмаларды қолдану, әдістемеге сәйкес Желілік агенттерді тағайындау керек және т.с.с.

Бағдарламалық жасақтаманы санаттау

Қолданбаларды іске қосуды бақылаудың негізгі құралы *Kaspersky* санаттары болып табылады (бұдан әрі *KL санаттар*). KL санаты Kaspersky Security Center әкімшісіне БЖ категориялауды қолдау жұмысын жеңілдетеді және басқарылатын құрылғыларға жіберілетін трафик көлемін барынша азайтады.

Реттелмелі санаттарды бірде-бір KL санатқа түспейтін бағдарламалар үшін ғана жасау керек (мысалы, тапсырысқа әзірленген бағдарламалар үшін). Реттелмелі санаттар бағдарламаның дистрибутиві (MSI) негізінде немесе дистрибутивтері бар қалтаның негізінде жасалады.

Егер KL санаттармен категорияланбаған бағдарламалық жасақтаманың үлкен толықтырылатын топтамасы болса, автоматты түрде жаңартылатын санатты жасаған жөн. Мұндай санат автоматты түрде дистрибутивтері бар қалтаны өзгерту кезінде орындалатын файлдардың бақылау сомаларымен толықтырылады.

Менің құжаттарым, %windir%, %ProgramFiles% және %ProgramFiles(x86)% қалталары үшін автоматты түрде жаңартылған бағдарламалық жасақтама санаттарын жасамаңыз. Бұл қалталардағы файлдар жиі өзгереді, бұл Басқару серверіне жүктемені ұлғайтуға және желідегі трафикті ұлғайтуға әкеледі. Бағдарламалық жасақтаманың топтамасы бар бөлек қалта жасау және оны кейде толықтыру керек.

Бірнеше қатысушысы бар бағдарламалар туралы

Kaspersky Security Center бағдарламасы провайдерлердің әкімшілеріне және клиенттердің әкімшілеріне көптиістілікті қолдайтын Kaspersky бағдарламаларын пайдалануға мүмкіндік береді. Провайдердің инфрақұрылымында Kaspersky бірнеше басқарушысы бар бағдарламасын орнатқаннан кейін, клиенттер бағдарламаны қолдана бастайды.

Әртүрлі клиентке қатысты тапсырмалар мен саясаттарды бөлу мақсатында, әрбір клиент үшін Kaspersky Security Center бағдарламасында жеке виртуалды Басқару серверін құру керек. Клиент үшін орындалатын бірнеше қатысушысы бар бағдарламаларға арналған барлық тапсырмалар мен саясаттар, осы клиентке сәйкес келетін виртуалды Басқару серверінің Басқарылатын құрылғылар басқару тобы үшін жасалуы керек. Негізгі Басқару серверіне қатысты басқару топтары үшін жасалған тапсырмалар клиент құрылғыларына әсер етпейді.

Провайдерлердің әкімшілерінен айырмашылығы, клиент әкімшісі тек тиісті клиент құрылғыларына арналған бағдарламалардың тапсырмалары мен саясаттарын құра алады және көре алады. Провайдердің әкімшілері мен клиент әкімшілеріне қолжетімді тапсырмалар мен саясат параметрлері әртүрлі. Кейбір тапсырмалар мен кейбір саясат параметрлері клиент әкімшілері үшін қолжетімді емес.

Клиенттің иерархиялық құрылымы ішінде бірнеше қатысушысы бар бағдарламалар үшін құрылған саясаттар ең төменгі деңгейдегі басқару топтары үшін де, ең жоғарғы деңгейдегі басқару топтары үшін де иленеді: саясат клиентке тиесілі барлық клиент құрылғыларына қатысты қолданылады.

Басқару сервері параметрлерін сақтық көшірмелеу және қалпына келтіру

Басқару серверінің параметрлерін және ол қолданатын дерекқорды сақтық көшірмелеу үшін сақтық көшірмелеу тапсырмасы және klbackup утилитасы қарастырылған. Сақтық көшірме Басқару серверінің барлық негізгі параметрлері мен нысандарын қамтиды: Басқару серверінің сертификаттары, басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері, лицензияларға арналған кілттер, барлық мазмұны, тапсырмалары, саясаттары және тағы басқасы бар басқару топтарының құрылымы. Сақтық көшірмеге ие болып, Басқару серверінің жұмысын аз уақытта - ондаған минуттан екі сағатқа дейін қалпына келтіруге болады.

Сақтық көшірме болмаса, ақау сертификаттардың және Басқару серверінің барлық параметрлерінің қайтарымсыз жоғалуына әкелуі мүмкін. Бұл Kaspersky Security Center қайтадан конфигурациялау, сондай-ақ ұйымның желісінде Желілік агентті бастапқы орналастыруды қайтадан орындау қажеттілігіне әкеледі. Сонымен қатар, басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері де жоғалады, бұл Kaspersky Endpoint Security-мен құрылғыларда шифрланған деректердің қайтарымсыз жоғалу қаупін тудырады. Сондықтан сақтық көшірудің штаттық тапсырмасы көмегімен Басқару серверінің сақтық көшірмелерін үнемі жасаудан бас тарту керек.

Жылдам іске қосу шебері басқару сервері параметрлерінің сақтық көшірме тапсырмасын жасайды және оны күнде 04:00-де іске қосылатындай орнатады. Сақтық көшірмелер әдепкісінше %ALLUSERSPROFILE%\Application Data\KasperskySC қалтасында сақталады.

Егер ДҚБЖ ретінде басқа құрылғыға орнатылған Microsoft SQL Server данасы қолданылса, сақтық көшірмелеу тапсырмасын өзгерту керек: жасалған сақтық көшірмелерді сақтау қалтасы ретінде Басқару серверінің қызметіне де, SQL Server қызметіне де жазу үшін қолжетімді UNC-жолын көрсету керек. Бұл талап Microsoft SQL Server ДҚБЖ үшін сақтық көшірмелеудің нәтижесі болып табылады.

Егер ДҚБЖ ретінде Microsoft SQL Server жергілікті данасы пайдаланылса, оларды бір уақытта Басқару серверімен зақымданудан қорғау үшін бөлек тасығышта сақтық көшірмелерді сақтау ұсынылады.

Сақтық көшірме маңызды деректерді қамтиды, сондықтан сақтық көшірмелеу тапсырмасында және klbackup утилитасында сақтық көшірмелерді құпиясөзбен қорғау қарастырылған. Әдепкі бойынша сақтық көшірмелеу тапсырмасы бос құпиясөзбен жасалады. Сақтық көшірмелеу сипаттарында құпиясөзді міндетті түрде белгілеу керек. Бұл талапты сақтамау Басқару серверінің сертификаттарының кілттері, лицензияларға арналған кілттер және басқарылатын құрылғылардың дисктерін шифрлау кілттері-шебері шифрланбаған болатынына әкеледі.

Үнемі сақтық көшірмелеумен қатар, барлық маңызды өзгерістердің алдында, соның ішінде Басқару серверін жаңа нұсқаға дейін жаңартудың алдында және Басқару серверінің патчтарын орнатудың алдында сақтық көшірмені жасау керек.

Егер ДҚБЖ ретінде Microsoft SQL Server қолдансаңыз, сіз сақтық көшірмелердің өлшемін барынша азайта аласыз. Бұл үшін SQL Server параметрлерінде **Сақтық көшірмелерді сығу (Compress backup)** жалаушасын орнатыңыз.

Сақтық көшірмеден қалпына келтіру klbackup утилитасы көмегімен сақтық көшірме жасалған нұсқадағы (немесе барынша жаңа) Басқару серверінің жаңа ғана орнатылған және жұмысқа қабілетті данасында орындалады.

Қалпына келтіру орындалатын Басқару серверінің инсталляциясы дәл сол немесе барынша жаңа нұсқадағы сондай түрдегі (мысалы, SQL Server немесе MariaDB) ДҚБЖ пайдалануы тиіс. Басқару серверінің нұсқасы сондай (ұқсас немесе барынша жаңа патчпен) немесе барынша жаңа болуы мүмкін.

Осы бөлімде параметрлерді және Басқару серверінің нысандарын қалпына келтірудің типтік сценарийлері сипатталған.

Басқару сервері бар құрылғы істен шықты

Егер ақау нәтижесінде Басқару сервері бар құрылғы істен шықса, келесі әрекеттерді орындау ұсынылады:

- Жаңа Серверге сол мекенжайды тағайындау: NetBIOS-атауы, FQDN-атауы, статикалық IP - Желілік агентті орналастырған кезде қайсысы белгіленгеніне байланысты.
- Сол немесе барынша жаңа нұсқада, сондай түрдегі ДҚБЖ қолдана отырып Басқару серверін орнату. Сол немесе барынша жаңа патчы бар Сервердің нұсқасын немесе барынша жаңа нұсқаны орнатуға болады. Орнатқан соң шебердің көмегімен бастапқы конфигурациялауды орындамаған жөн.
- **Іске қосу** мәзірінен klbackup сақтық көшірмелеу утилитасын іске қосыңыз және қалпына келтіруді орындаңыз.

Басқару серверінің параметрлері немесе дерекқор зақымдалған

Егер Басқару сервері параметрлердің немесе дерекқордың зақымдалуы нәтижесінде жұмысқа қабілетсіз болса (мысалы, қуат ақаулығы себебінен), қалпына келтірудің келесі сценарийін қолдану ұсынылады:

1. Зақымданған құрылғыда файлдық жүйені тексеруді орындау.
2. Басқару серверінің жұмысқа қабілетсіз нұсқасын деинсталляциялау.
3. Сол түрдегі, сол немесе барынша жаңа нұсқадағы ДҚБЖ қолдана отырып Басқару серверін қайтадан орнату. Сол немесе барынша жаңа патчы бар Сервердің нұсқасын немесе барынша жаңа нұсқаны орнатуға болады. Орнатқан соң шебердің көмегімен бастапқы конфигурациялауды орындамаған жөн.
4. **Іске қосу** мәзірінен klbackup сақтық көшірмелеу утилитасын іске қосыңыз және қалпына келтіруді орындаңыз.

Басқару серверін klbackup штаттық утилитасынан басқа кез келген тәсілмен қалпына келтіруге болмайды.

Серверді бөтен бағдарламалық жасақтаманың көмегімен қалпына келтірудің барлық жағдайларында Kaspersky Security Center таратылған бағдарламасының түйіндерінде деректердің синхронизациясы бұзылады.

Желілік агент пен қауіпсіздік бағдарламасын орналастыру

Ұйымның құрылғыларын басқару үшін құрылғыларға Желілік агентті орнату қажет. Ұйымның құрылғыларында Kaspersky Security Center таратылған қолданбасын орналастыру әдетте оларға Желілік агентті орнатудан басталады.

Microsoft Windows XP-де Желілік агент келесі операцияларды дұрыс емес орындауы мүмкін: жаңартуларды тікелей Kaspersky серверлерінен жүктеп алу (егер тарату нүктесінің рөлін орындаса); KSN прокси-сервері ретінде жұмыс істеу (егер тарату нүктесінің рөлін орындаса); және үшінші тараптардың бағдарламаларының осалдықтарын анықтау (Осалдықтар мен патчтарды басқаруды қолданған кезде).

Бастапқы орналастыру

Егер құрылғыда Желілік агент әлдеқашан орнатылған болса, мұндай құрылғыға бағдарламаларды қашықтан орнату Желілік агенттің көмегімен жүзеге асырылады. Бұл ретте, орнатылатын бағдарламаның дистрибутивін әкімші көрсеткен орнату параметрлерімен бірге жіберу, Желілік агенттер мен Басқару сервері арасындағы байланыс арналары арқылы жүзеге асырылады. Дистрибутивті жіберу үшін тарату нүктелері, көп мекенжайлы таратылым және басқа да құралдар түріндегі аралық тарату орталықтарын пайдалануға болады. Бағдарламаларды Желілік агенті орнатылған басқарылатын құрылғыларға орнату туралы толығырақ мәліметті одан әрі осы бөлімде қараңыз.

Желілік агентті Microsoft Windows платформасындағы құрылғыларға бастапқы орнатуды келесі тәсілдермен орындауға болады:

- Бағдарламаларды қашықтан орнатудың үшінші тарап құралдары арқылы.
- Windows топтық саясаттары арқылы: топтық саясаттар үшін Windows стандартты басқару құралдарын қолдану.
- Kaspersky Security Center бағдарламаларын қашықтан орнату тапсырмасындағы тиісті параметрлердің көмегімен мәжбүрлі түрде.
- Пайдаланушыларға Kaspersky Security Center қалыптастырған автономды пакеттерге сілтемелер тарату арқылы. Автономды пакеттер, параметрлері конфигурацияланған таңдалған бағдарламалардың дистрибутивтерін қамтитын орындалатын модульдер болып табылады.
- Құрылғыларда бағдарламалардың инсталляторларын іске қосу арқылы қолмен.

Microsoft Windows-тен ерекшеленетін платформаларда, Желілік агентті басқарылатын құрылғыларда бастапқы орнату, қолда бар үшінші тарап құралдарымен немесе пайдаланушыларға алдын ала конфигурацияланған дистрибутиві бар мұрағаты жіберу арқылы қолмен жүзеге асырылуы керек. Желілік агентті жаңа нұсқасына дейін жаңарту, сондай-ақ Kaspersky басқа бағдарламаларын осы платформаларға бағдарламаларды қашықтан орнату тапсырмаларының көмегімен, құрылғылардағы Желілік агенттерді қолдану арқылы орнату. Бұл жағдайда, орнату Microsoft Windows платформасында орнатуға ұқсас жолмен жүзеге асырылады.

Басқарылатын желіде бағдарламаларды орналастыру тәсілі мен стратегиясын таңдай отырып, бірқатар факторларды назарға алған жөн (тізімі толық емес):

- Ұйым желісінің конфигурациясын
- Құрылғылардың жалпы санын
- Басқарылатын желіде Windows домендерінің болуы, осындай домендерде Active Directory топтық саясаттарына өзгерістер енгізу мүмкіндігі
- Kaspersky бағдарламаларын бастапқы орналастыру жүргізілетін құрылғыларда жергілікті әкімші құқықтары бар есептік жазбаны (жазбаларды) білу (яғни, жергілікті әкімші құқықтары бар домендік есептік жазбаның қолжетімді болуы немесе осындай құрылғыларда әкімші құқықтары бар бірегейлендірілген жергілікті есептік жазбалардың болуы)
- Басқару сервері мен MSP клиенттерінің желілері арасындағы байланыс сипаты мен желілік арналардың ені және осы желілердегі желілік арналардың ені
- Орналастыру басталған сәтте қашықтағы құрылғыларда қолданылатын қауіпсіздік параметрлері (атап айтқанда, UAC және Simple File Sharing режимін пайдалану)

Инсталляторлар параметрлерін конфигурациялау

Kaspersky бағдарламаларын желіге орналастыруға кіріспес бұрын, орнату параметрлерін – бағдарламаны орнату барысында конфигурацияланатын параметрлерді анықтап алу керек. Желілік агентті орнатқан кезде, ең болмағанда, Басқару серверіне қосылуға арналған мекенжайды, proxy параметрлерін және бәлкім, кейбір қосымша параметрлерді белгілеу қажет. Таңдалған орнату тәсіліне байланысты, параметрлерді әртүрлі тәсілдермен белгілеуге болады. Ең қарапайым жағдайда (таңдалған құрылғыға қолмен интерактивті түрде орнатылған кезде), қажетті параметрлерді инсталлятордың пайдаланушы интерфейсі арқылы белгілеуге болады, осылайша кейбір жағдайларда бастапқы орналастыру тіпті пайдаланушыларға инсталлятор интерфейсінде енгізуі тиіс болатын параметрлерді (Басқару сервері мекенжайлары және т.с.с.) көрсету арқылы Желілік агенттің дистрибутивіне сілтеме жіберу арқылы жүзеге асырылуы да мүмкін.

Параметрлерді конфигурациялаудың бұл тәсілі пайдаланушылар үшін қолайсыз болғандықтан және олардың параметрлерді қолмен белгілеуіндегі қателіктер туындауының жоғары ықтималдығына байланысты, тәжірибеде қолдануға ұсынылмайды және құрылғылар тобына бағдарламаларды тыныш орнатуға жарамайды. Әдеттегі жағдайда, әкімші алдағыда автономды пакеттерді қалыптастыру үшін пайдаланылуы мүмкін параметрлердің мәндерін орталықтандырылған түрде көрсетуі керек. Автономды пакеттер, әкімші белгілеген параметрлері бар дистрибутивтердің өздігінен ашылатын мұрағаттары болып саналады. Автономды пакеттер, соңғы пайдаланушылардың жүктеп алуы үшін және желідегі таңдалған құрылғыларға тыныш тәсілмен орнатуы үшін қолжетімді ресурстарда (мысалы, Kaspersky Security Center веб-серверінде) орналастырылуы мүмкін.

Орнату пакеттері

Қолданбаларды орнату параметрлерін конфигурациялаудың бірінші және негізгі тәсілі әмбебап болып табылады және қолданбаларды орнатудың барлық тәсілдеріне жарамды болып келеді: Kaspersky Security Center құралдарымен де, үшінші тарап құралдарының көпшілігі көмегімен де. Бұл тәсіл Kaspersky Security Center-де қолданбалардың орнату пакеттерін құруды білдіреді.

Орнату пакеттері келесі тәсілдермен жасалады:

- көрсетілген дистрибутивтерден, олардың құрамына кіретін *сипаттауыштар* негізінде автоматты түрде (орнату және нәтижені талдау ережелерін және басқа ақпаратты қамтитын kud кеңейтімі бар файлдар);

- инсталляторлардың немесе Microsoft Windows Installer (MSI) пішіміндегі инсталляторлардың орындалатын файлдарынан – стандартты немесе қолдау көрсетілетін қолданбалар үшін.

Жасалған орнату пакеттері ішкі қалталары мен файлдары салынған қалталар болып саналады. Бастапқы дистрибутивтен басқа, орнату пакеті өңделетін параметрлерді (инсталлятордың өзінің параметрлерін және орнатуды аяқтау үшін операциялық жүйені қайта іске қосу қажеттілігі сияқты жағдайларды өңдеу ережелерін қоса), сондай-ақ шағын көмекші модульдерді қамтиды.

Белгілі бір қолдау көрсетілетін қолданбаға тән орнату параметрлерінің мәндері, орнату пакетін жасау кезінде Басқару консолінің пайдаланушы интерфейсінде белгілеуге болады (конфигурациялаудың одан да көп параметрлері әлдеқашан жасалған орнату пакетінің сипаттарында қолжетімді болуы мүмкін). Бағдарламаларды Kaspersky Security Center құралдарымен қашықтан орнатқан жағдайда, орнату пакеттері бағдарлама инсталляторын іске қосқан кезде оған әкімші белгілеген барлық параметрлер қолжетімді болатындай етіп құрылғыға жеткізіледі. Kaspersky бағдарламаларын орнатудың үшінші тарап құралдарын пайдаланған кезде құрылғыда бүкіл орнату пакетінің, яғни дистрибутив пен оның параметрлерінің болуын қамтамасыз ету жеткілікті. Орнату пакеттері Kaspersky Security Center тарапынан жалпы деректер каталогының тиісті қалтасында жасалады және сақталады.

Орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетпеңіз.

Үшінші тарап құралдарымен орналастырмас бұрын, Kaspersky бағдарламалары үшін параметрлерді конфигурациялаудың осы тәсілін қалай қолдануға болатындығы туралы "Microsoft Windows топтық саясаттар механизмі көмегімен орналастыру" бөлімінен қараңыз.

Kaspersky Security Center орнатылғаннан кейін, бірден орнатуға дайын бірнеше орнату пакеттері, соның ішінде Microsoft Windows платформасына арналған Желілік агент пакеттері мен қауіпсіздік бағдарламалары автоматты түрде жасалады.

MSP клиентінің желісіне қолданбаларды орналастыру үшін орнату пакеттерін пайдалану, кейбір жағдайларда MSP клиенттеріне сәйкес келетін виртуалды Серверлерде орнату пакеттерін жасау қажеттілігін білдіреді. Виртуалды Серверлерде орнату пакеттерін жасау, әртүрлі MSP клиенттері үшін орнату пакеттерінде орнатудың әртүрлі параметрлерін пайдалануға мүмкіндік береді. Бұл, ең алдымен, Желілік агенттің орнату пакеттерінде қажет, өйткені әртүрлі MSP клиенттерінің желілерінде орналастырылған Желілік агенттер Басқару серверіне қосылудың әр түрлі мекенжайларын қолданады. Шын мәнінде, байланыстың мекенжайы және Желілік агенттің қандай виртуалды Серверге қосылатынын анықтайды.

Виртуалды Серверде тікелей жаңа орнату пакеттерін жасау мүмкіндігіне ие болумен қатар, виртуалды Серверлерде орнату пакеттерімен жұмыс істеудің негізгі режимі – негізгі Сервердің орнату пакеттерін виртуалды Серверге тарату болып табылады. Таңдалған (немесе барлық) пакеттерді таңдалған виртуалды Серверлерге (соның ішінде таңдалған басқару тобына кіретін барлық Серверлерге) тиісті Басқару сервері тапсырмасы арқылы таратуға болады. Жаңа виртуалды Серверді жасау кезінде, шеберді негізгі Сервердің орнату пакеттерінің тізімін таңдауға болады. Таңдалған пакеттер жаңадан жасалған виртуалды Серверге бірден таралады.

Орнату пакетін тарату кезінде, оның ішіндегісі толығымен көшірілмейді. Виртуалды Серверде таратылған орнату пакетіне сай келетін файл қоймасында, осы виртуалды Серверге тән параметр файлдары ғана сақталады. Орнату пакетінің негізгі, өзгеріссіз бөлігі (орнатылатын қолданбаның дистрибутивін қоса) тек негізгі Сервердің қоймасында ғана сақталады. Бұл, жүйенің өнімділігін айтарлықтай арттыруға және қажетті дискілік кеңістіктің көлемін азайтуға мүмкіндік береді. Виртуалды Серверлерге таратылған орнату пакеттерімен жұмыс істеу кезінде (яғни қашықтан орнату тапсырмаларын жұмыс істеген кезде немесе жеке орнату пакеттерін жасау кезінде), виртуалды Серверде таралған пакетке сай келетін параметрлері бар файлдар мен негізгі Сервердің бастапқы орнату пакетіндегі деректер "қосылады".

Бағдарламаға арналған лицензиялық кілтті орнату пакетінің сипаттарында белгілеуге болатынына қарамастан, осы лицензия тарату тәсілін қолданбаған жөн, себебі қалтадағы файлдарға қатынасу мүмкіндігін кездейсоқ алып, оларды оқып қоюға болады. Автоматты түрде таратылған лицензиялық кілттерді немесе лицензиялық кілттерді орнату тапсырмаларын қолданған жөн.

MSI сипаттары және түрлендіру файлдары

Windows платформасында орнату параметрлерін конфигурациялаудың тағы бір тәсілі, MSI және түрлендіру файлдарының сипаттарын белгілеу. Бұл тәсіл, Microsoft Installer пішіміндегі инсталляторлармен жұмыс істеуге бағытталған үшінші тарап құралдарының көмегімен орнату кезінде, сондай-ақ Windows топтық саясаттары арқылы Microsoft штаттық құралдарының көмегімен немесе Windows топтық саясаттарымен жұмыс істеуге арналған басқа да үшінші тарап құралдарының көмегімен орнату кезінде қолданылуы мүмкін.

Қолданбаларды қашықтан орнатудың үшінші тарап құралдары арқылы орналастыру

Егер ұйымда қолданбаларды қашықтан орнатудың кез келген құралы болса (мысалы, Microsoft System Center), осы құралдардың көмегімен бастапқы орналастыруды жүзеге асырған жөн.

Келесі әрекеттерді орындау керек:

- Қолданылатын орналастыру құралы үшін ең қолайлы орнату параметрлерін конфигурациялау тәсілін таңдау.
- Басқару консолі интерфейсі арқылы орнату пакеттерінің параметрлерін өзгерту және осы орнату пакеттерінен қолданбаларды орналастырудың таңдалған үшінші тарап құралдарының жұмысы арасындағы синхрондау механизмін анықтау.

Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмалары туралы жалпы мәліметтер

Kaspersky Security Center бағдарламасы, қолданбаларды қашықтан орнату тапсырмалары ретінде іске асырылатын қолданбаларды қашықтан орнатудың әртүрлі механизмдерін ұсынады. Қашықтықтан орнату тапсырмасын көрсетілген басқару тобы үшін де, құрылғылар жиынтығы үшін де немесе құрылғыларды таңдау үшін де жасауға болады (мұндай тапсырмалар **Тапсырмалар** қалтасындағы Басқару консолінде көрсетіледі). Тапсырманы жасау кезінде, сіз осы тапсырманы пайдаланып, орнатылатын орнату пакеттерін (Желілік агент және/немесе басқа қолданба) таңдай аласыз, сонымен қатар қашықтан орнату тәсілін анықтайтын бірқатар параметрлерді орната аласыз.

Басқару топтарына арналған тапсырмалар тек осы топқа жататын құрылғыларда ғана емес, таңдалған топтың барлық ішкі топтарының барлық құрылғыларында да жұмыс істейді. Егер тапсырма параметрлерінде тиісті параметр қосылса, тапсырма осы топта немесе оның ішкі топтарында орналасқан қосалқы Басқару серверлерінің құрылғыларына қолданылады.

Құрылғылар жиынтығына арналған тапсырмалар, тапсырманы іске қосу кезінде құрылғыларды таңдау құрамына сәйкес әрбір рет іске қосу кезінде клиент құрылғыларының тізімін жаңартады. Егер құрылғыларды таңдауда қосалқы Басқару серверлеріне қосылған құрылғылар болса, тапсырма осы құрылғыларда да іске қосылады.

Басқару серверлеріне қосылған құрылғыларда қашықтан орнату тапсырмасының сәтті жұмыс істеуі үшін, тапсырма пайдаланатын орнату пакеттерін тарату тапсырмасының көмегімен тиісті қосалқы Басқару серверлеріне алдын ала тарату керек.

Microsoft Windows топтық саясаттары тетігінің көмегімен орналастыру

Желілік агенттерді бастапқы орналастыруды, келесі шарттарды орындаған кезде Microsoft Windows топтық саясаттарының көмегімен жүзеге асырылған жөн:

- құрылғылар Active Directory доменінің мүшелері;
- Active Directory топтық саясаттарын жасауға және түрлендіруге мүмкіндік беретін әкімші құқықтарымен домен контроллеріне қатынасуға рұқсат берілген;
- конфигурацияланған орнату пакеттерін басқарылатын құрылғылар желісіне (барлық құрылғылар үшін оқуға қолжетімді ортақ қатынасы бар қалтаға) көшіру мүмкіндігі бар;
- орналастыру жоспары, Желілік агенттерді орналастыра бастауға дейін құрылғылардың штаттық жағдайда қайта іске қосылуын күте тұруға мүмкіндік береді немесе құрылғыларға Windows топтық саясатын күшпен қолдануға болады.

Осы орналастыру тәсілінің мәні келесіде:

- Microsoft Installer пішіміндегі қолданбаның дистрибутив бумасы (MSI пакеті) ортақ қатынасы бар қалтада орналастырылады (құрылғылардың LocalSystem есептік жазбалары оқуға қатынасу мүмкіндігі бар қалтада).
- Active Directory топтық саясатында осы дистрибутивті орнату нысаны жасалады.

- Орнатудың әрекет ету ауқымы ұйымдық бөлімшеге және/немесе құрылғыларды қамтитын қауіпсіздік тобына байлау арқылы белгіленеді.

- Құрылғының доменге кезекті кіруі кезінде (жүйеге құрылғы пайдаланушылар кіргенге дейін) орнатылған қолданбалар арасында қажетті қолданбаның болуын тексеру орындалады. Қолданба болмаса, дистрибутив саясатта белгіленген ресурстан жүктеп алынып, орнатылады.

Осы орналастыру тәсілінің артықшылықтарының бірі, тағайындалған қолданбалар, пайдаланушы жүйеге кірмес бұрын, операциялық жүйені жүктеу кезінде құрылғыларға орнатылады. Тіпті қажетті құқықтары бар пайдаланушы қолданбаны жойса да, операциялық жүйені келесі жолы жүктеу кезінде, ол қайтадан орнатылады. Осы орналастыру тәсілінің кемшілігі, әкімші тарапынан топтық саясатта жүзеге асырылған өзгерістер құрылғыны қайта іске қоспайынша күшіне енбейді (қосымша құралдарды қолданбай).

Топтық саясаттардың көмегімен, Желілік агентті де, инсталляторлары Windows Installer пішіміне ие басқа қолданбаларды да орнатуға болады.

> MSI пакетінен желілік агентті тек тыныш режимде орнатуға болады, MSI пакетінен интерактивті орнатуға қолдау көрсетілмейді.

Осы орналастыру тәсілін таңдау кезінде, бұдан бөлек, Windows топтық саясатын қолдану кезінде құрылғыға файлдар көшірілетін файлдық ресурсқа түсетін жүктемені бағалау керек. Сондай-ақ, конфигурацияланған орнату пакетін осы ресурсқа жеткізу тәсілін және орнату пакетінің параметрлеріндегі тиісті өзгерістерді синхрондау әдісін таңдау керек.

Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасының көмегімен Microsoft Windows саясаттарымен жұмыс істеу

Осы орналастыру тәсілі, құрылғылар кіретін домен контроллеріне Басқару сервері орнатылған құрылғыдан қатынасу мүмкін болғанда, ал құрылғылардан – Басқару серверінің ортақ қатынас бар қалтасы (орнату пакеттері орналасқан) оқу үшін қолжетімді болғанда ғана жүзеге асырылуы ықтимал. Сол себепті, осы орналастыру тәсілі MSP мәнмәтінінде қарастырылмайды.

Қолданбаларды Microsoft Windows саясаттары көмегімен өз бетінше орнату

Әкімші Windows топтық саясатында орнату үшін қажетті нысандарды өз бетінше жасай алады. Бұл жағдайда, пакеттерді бөлек файл серверіне жүктеп, оларға сілтеме жасау керек.

Келесі орнату сценарийлері жүзеге асырылуы мүмкін:

- Әкімші орнату пакетін жасап, оның сипаттарын Басқару консолінде конфигурациялайды. Содан соң, әкімші осы пакеттің EXEC ішкі қалтасын Kaspersky Security Center ортақ қатынасы бар қалтасынан ұйымның мамандандырылған файл ресурсындағы қалтаға толығымен көшіріп алады. Топтық саясат нысаны, ұйымның мамандандырылған файл ресурсындағы ішкі қалтада жатқан осы пакеттің MSI файлына сілтеме жасайды.

- Әкімші интернеттен қолданбаның дистрибутивін (оның ішінде Желілік агенттің дистрибутивін) жүктеп алады және оны ұйымның мамандандырылған файл ресурсына жүктейді. Топтық саясат нысаны, ұйымның мамандандырылған файл ресурсындағы ішкі қалтада жатқан осы пакеттің MSI файлына сілтеме жасайды. Орнату параметрлерін конфигурациялау MSI сипаттарын конфигурациялау немесе MST түрлендіру файлдарын конфигурациялау арқылы жүзеге асырылады.

Kaspersky Security Center қолданбаларын қашықтан орнату тапсырмасы арқылы мәжбүрлеп орналастыру

Желілік агентті немесе басқа бағдарламаларды бастапқы енгізу үшін әрбір құрылғыда жергілікті әкімші құқықтары бар пайдаланушы есептік жазбалары болған жағдайда, Kaspersky Security Center қашықтан орнату тапсырмасымен таңдалған орнату пакеттерін мәжбүрлі түрде орнатуға болады.

Күшпен орнату құрылғылар тікелей Басқару серверіне қолжетімді болмаған жағдайда қолданылуы мүмкін: мысалы, құрылғылар оқшауланған желілерде орналасқан немесе құрылғылар жергілікті желіде, ал Басқару сервері - демилитаризацияланған аймақта орналасқан.

Бастапқы енгізу кезінде желілік агент орнатылмайды. Сондықтан қашықтан орнату тапсырмасының параметрлерінде Желілік агент көмегімен қолданбаны орнату үшін қажетті файлдарды таратуды таңдау мүмкін емес. Файлдарды басқару сервері немесе тарату нүктесі көмегімен операциялық жүйе ресурстарын пайдаланып қана тарата аласыз.

Басқару серверінің қызметі мақсатты құрылғыларда әкімші құқықтары бар есептік жазбамен іске қосылуы керек. Сондай-ақ қашықтан орнату тапсырмасы параметрлерінде admin$ жалпы қатынасы бар әкімшілік ресурстарына кіре алатын есептік жазбаны көрсетуге болады.

Әдепкі бойынша қашықтан орнату тапсырмасы құрылғыларға басқару сервері іске қосылған есептік жазбаның (яғни admin$ ортақ орнына кіруге арналған есептік жазба) кіру деректерін пайдаланып қосылады. Бұл тіркелгіні қашықтан орнату тапсырмасының баптауларында нысаналы құрылғыларда Желілік агент орнатылмаған жағдайда ғана көрсету керек.
Linux негізіндегі құрылғыларда орындалатын қашықтан орнату тапсырмасын жасау кезінде SSH қосылымын орнату үшін әрқашан тіркелгіні көрсету керек.

Мақсатты құрылғыларды олар тиесілі Kaspersky Security Center басқару тобын таңдау немесе белгілі бір шартқа негізделген құрылғылар таңдауын жасау арқылы анық (тізімде) көрсетуге болады. Орнатуды іске қосу уақыты тапсырма кестесімен анықталады. Тапсырманың сипаттарында **Өткізіп алынған тапсырмаларды іске қосу** параметрі қосулы болса, тапсырма құрылғыларды қосу кезінде немесе оларды мақсатты басқару тобына көшіру кезінде бірден іске қосылуы мүмкін.

Мәжбүрлеп орнату әрекеті, орнату пакеттерін мақсатты құрылғыларға жеткізу, содан соң файлдарды құрылғылардың әрқайсысының admin$ басқару ресурсына көшіру және оларға көмекші қызметтерді қашықтан тіркеу арқылы жүзеге асырылады. Орнату пакеттерін мақсатты құрылғыларға жеткізу әрекеті, желілік өзара әрекеттесуге жауап беретін Kaspersky Security Center функциясы арқылы жүзеге асырылады. Бұл жағдайда, келесі шарттар орындалуы керек:

- Мақсатты құрылғыларға басқару серверінен немесе тарату нүктесінен қол жеткізуге болады.
- Желіде құрылғыларға арналған атаулар рұқсаты дұрыс жұмыс істеп жатыр.
- Мақсатты құрылғыларда admin$ жалпы қатынасын басқару ресурстары қосулы.
- Мақсатты құрылғыларда келесі жүйелік қызметтер іске қосылған:
  - Сервер (LanmanServer).

    Әдепкі бойынша бұл қызмет іске қосылған.
  - DCOM Server Process Launcher (DcomLaunch).

- RPC Endpoint Mapper (RpcEptMapper).
- Қашықтағы процедураны шақыру (Remote Procedure Call, RpcSs).

- TCP 445 порты Windows құралдары көмегімен қашықтан қол жеткізуге рұқсат беру үшін мақсатты құрылғыларда ашық.

  > TCP 139, UDP 137 және UDP 138 ескі протоколдармен пайдаланылады және енді ағымдағы бағдарламаларға қажет емес.

  Басқару серверін және тарату нүктелерін мақсатты құрылғыларға қосу үшін желілік экранда динамикалық шығыс кіру порттарына рұқсат берілуі керек.

- Желілік агентті енгізу кезінде Active Directory домен саясатының қауіпсіздік параметрлерінде NTLM протоколының жұмысын қамтамасыз етуге рұқсат берілді.
- Microsoft Windows XP басқаратын мақсатты құрылғыларда Simple File Sharing режимі өшірулі.
- Мақсатты құрылғыларда *классикалық бөлісу және қауіпсіздік моделінің параметрлері орнатылған — жергілікті пайдаланушылар өздерін аутентификациялайды.* Мұндай модель *тек қонақ болуы мүмкін емес – жергілікті пайдаланушылар қонақ ретінде аутентификациялайды.*
- Құрылғылар домен мүшелері болып табылады немесе құрылғыларда басқару құқықтары бар бірегейлендірілген есептік жазбалар алдын ала жасалған.

> Windows Server 2003 немесе одан жоғары операциялық жүйе нұсқасы орнатылған Active Directory доменіне қосылмаған құрылғыда желілік агент немесе басқа бағдарламаларды сәтті енгізу үшін сол құрылғыда қашықтағы UAC өшіру керек. Қашықтағы UAC — жергілікті әкімші есептік жазбаларының admin$-ке қол жеткізе алмауы себептерінің бірі, бұл желілік агентті және басқа бағдарламаларды мәжбүрлі түрде енгізу үшін қажет. Қашықтағы UAC өшіру жергілікті UAC-ге әсер етпейді.

Kaspersky Security Center басқару топтарында әлі орналастырылмаған жаңа құрылғыларға орнатқан кезде, қашықтан орнату тапсырмасының сипаттарында Желілік агентті орнату аяқталғаннан кейін құрылғылар көшірілетін басқару тобын белгілеуге болады.

> Топтық тапсырманы жасау кезінде, топтық тапсырма таңдалған топтың барлық салынған ішкі топтарының құрылғыларына әсер ететінін есте ұстаған жөн. Сондықтан, орнату тапсырмаларын ішкі топтарда қайталамау керек.

Бағдарламаларды мәжбүрлі түрде орнату үшін тапсырмаларды жасаудың жеңіл жолы — автоматты түрде орнату. Ол үшін басқару тобының сипаттарында орнату пакеттерінің тізімін ашып, осы топтың құрылғыларына орнатылуы керек пакеттерді таңдау керек. Нәтижесінде, осы топтың және оның ішкі топтарының барлық құрылғыларында, таңдалған орнату пакеттері автоматты түрде орнатылады. Пакеттер орнатылатын кезең, желінің өткізу қабілетіне және желідегі құрылғылардың жалпы санына байланысты.

Орнату пакеттерін мақсатты құрылғыларға тарату кезінде басқару серверіндегі жүктемені азайту үшін орнату тапсырмасында тарату нүктелерін пайдаланып, орнатуды таңдауға болады. Орнатудың бұл тәсілі, тарату нүктелерімен тағайындалған құрылғыларға елеулі жүктеме түсіретінін ескеру қажет. Тарату нүктелеріне қойылатын талаптарға сай құрылғыларды таңдау ұсынылады. Тарату нүктелерін пайдалансаңыз, олардың мақсатты құрылғыларды орналастыратын оқшауланған ішкі желілердің әрқайсысында болуын қамтамасыз ету керек.

Жергілікті орнату орталықтары ретінде тарату нүктелерін қолдану ішкі желі ішінде құрылғылар арасында кең байланыс арнасы бар болған кезде тар байланыс арнасымен Басқару серверіне қосылған ішкі желілерде құрылғыларға орнату үшін де ыңғайлы болуы мүмкін.

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit қалтасы бар бөлімде бос орын көлемі орнатылатын бағдарламалар дистрибутивтерінің жиынтық көлемінен бірнеше есе асып кетуі қажет.

Kaspersky Security Center қалыптастырған автономды пакеттерді іске қосу

Желілік агент пен қолданбаларды бастапқы орналастырудың жоғарыда сипатталған тәсілдері барлық қажетті шарттарды орындай алмағандықтан, жүзеге аса бермеуі мүмкін. Мұндай жағдайларда, Kaspersky Security Center құралдарымен орнатудың қажетті параметрлері бар әкімші дайындаған орнату пакеттерінен *жеке орнату пакеті* деп аталатын бірыңғай орындалатын файл жасауға болады. Мұның мәні болса (Веб-серверге құрылғы пайдаланушылары үшін сырттан қатынасу конфигурацияланған), жеке орнату пакеті ішкі Веб-серверде (Kaspersky Security Center құрамына кіретін), сондай-ақ Kaspersky Security Center Web Console құрамына кіретін арнайы орналастырылған Веб-серверде жариялануы мүмкін. Автономды пакеттерді басқа Веб-серверге де көшіруге болады.

Kaspersky Security Center бағдарламасының көмегімен, таңдалған пайдаланушыларға қолданылып жатқан Веб-сервердегі автономды пакет файлына сілтемені электрондық пошта арқылы (интерактивті түрде немесе "тыныш" орнату "-s" кілтімен) файлды іске қосу туралы өтінішпен бірге таратуға болады. Жеке орнату пакетін, Веб-серверге қатынаса алмайтын құрылғыларды пайдаланушылар үшін электрондық пошта хабаррына тіркеуге болады. Сонымен қатар, әкімші автономды пакетті сыртқы құрылғыға көшіре алады және пакетті кейіннен іске қосу мақсатымен қажетті құрылғыға жеткізе алады.

Автономды пакетті Желілік агент пакетінен, басқа қолданба пакетінен (мысалы, қауіпсіздік бағдарламасынан) немесе бірден екі пакеттен де жасауға болады. Егер автономды пакет Желілік агент пен басқа қолданбадан жасалса, онда орнату Желілік агенттен басталады.

Желілік агентпен автономды пакетті жасау кезінде, Желілік агентті орнату аяқталғаннан кейін жаңа құрылғылар (бұрын басқару топтарында орналастырылмаған) автоматты түрде көшірілетін басқару тобын көрсетуге болады.

Автономды пакеттер интерактивті түрде (әдепкі бойынша), оларға кіретін қолданбаларды орнату нәтижесін көрсете отырып немесе "тыныш" режимде ("-s" кілтімен іске қосылғанда) жұмыс істей алады. "Тыныш" режимді кез келген скрипттерден орнату үшін пайдалануға болады (мысалы, операциялық жүйенің кескінін орналастыру аяқталғаннан кейін іске қосылатын скрипттерден және т.с.с.). "Тыныш" режимде орнату нәтижесі процесті қайтару кодымен анықталады.

Қолданбаларды қолмен басқару мүмкіндіктері

Әкімшілер немесе тәжірибелі пайдаланушылар қолданбаларды интерактивті режимде қолмен орната алады. Бұл арада, сіз Kaspersky Security Center ортақ қатынасы бар қалтасында орналасқан бастапқы дистрибутивтерді де, олардан құрылған орнату пакеттерін де пайдалана аласыз. Инсталляторлар әдепкі бойынша интерактивті режимде жұмыс істейді, пайдаланушыдан барлық қажетті параметр мәндерін сұрайды. Бірақ "-s" кілті бар орнату пакетінің түбірінен setup.exe процесін іске қосқан кезде, инсталлятор орнату пакетін реттеген кезде белгіленген параметрлермен "тыныш" режимде жұмыс істейді.

Орнату пакетінің түбірінен setup.exe іске қосылған кезде, алдымен пакет уақытша жергілікті қалтаға көшіріледі, содан кейін қолданба инсталляторы жергілікті қалтадан іске қосылады.

Желілік агенті орнатылған құрылғыларға бағдарламаларды қашықтан орнату

Егер құрылғыда негізгі Басқару серверіне немесе оның қосалқы Серверлерінің біріне қосылған жұмысқа жарамды Желілік агент орнатылған болса, онда осы құрылғыда Желілік агенттің нұсқасын жаңартуға, сондай-ақ Желілік агенттің көмегімен кез келген қолдау көрсетілетін қолданбаларды орнатуға, жаңартуға немесе жоюға болады.

Бұл функция **қолданбаларды қашықтан орнату тапсырмасының** сипаттарында Желілік агенттің көмегімен жалаушасы арқылы қосылады.

Жалауша қойылған болса, құрылғыларға әкімші белгілеген орнату параметрлері бар орнату пакеттерін жіберу, Желілік агент пен Басқару сервері арасындағы байланыс арналары арқылы жүзеге асырылады.

Басқару серверіне түсетін жүктемені оңтайландыру және Басқару сервері мен құрылғылар арасындағы трафикті азайту үшін, әрбір қашықтағы желіде немесе әрбір кеңінен тарататын доменде тарату нүктелерін тағайындаған жөн ("Тарату нүктелері туралы" және "Басқару топтары құрылымын құру және тарату нүктелерін тағайындау" бөлімдерін қараңыз). Бұл жағдайда, орнату пакеттері мен инсталлятор параметрлерін тарату, құрылғыларға Басқару серверінен тарату нүктелері арқылы жүзеге асырылады.

Сондай-ақ, тарату нүктелерін қолдана отырып, бағдарламаларды орналастыру барысында желілік трафикті бірнеше есе төмендетуге мүмкіндік беретін орнату пакеттерін кеңінен (көп мекенжайға) таратуға болады.

Орнату пакеттерін құрылғыларға Желілік агенттер мен Басқару сервері арқылы байланыс арналары бойынша жіберу кезінде, жіберуге дайындалған орнату пакеттері %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer қалтасында қосымша түрде кэштеледі. Үлкен өлшемдегі әртүрлі орнату пакеттерінің көп бөлігін қолдану кезінде және тарату нүктелерінің көп санында осы қалтаның өлшемі айтарлықтай ұлғаюы мүмкін.

FTServer қалтасындағы файлдарды жоюға болмайды. Бастапқы орнату пакеттерін жою кезінде, тиісті деректер FTServer қалтасынан да автоматты түрде жойылатын болады.

Тарату нүктелері жағында қабылданатын деректер %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp қалтасында сақталады.

$FTCITmp қалтасындағы файлдарды жоюға болмайды. Қалтадағы деректерді қолданатын тапсырмаларды аяқтау шамасына қарай, осы қалтаның ішіндегісі автоматты түрде жойылады.

Орнату пакеттері, желі арқылы беру үшін оңтайландырылған аралық қоймадан Басқару сервері мен Желілік агент арасындағы байланыс арналары бойынша таратылатындықтан, орнату пакетінің бастапқы қалтасындағы орнату пакеттеріне өзгеріс енгізуге болмайды. Мұндай өзгерістерді Басқару сервері автоматты түрде ескермейді. Орнату пакеттерінің файлдарын қолмен өзгерту қажет болса (мұны жасау ұсынылмайды), Басқару консоліндегі орнату пакетінің қандай да бір параметрлерін міндетті түрде өзгерту керек. Басқару консоліндегі орнату пакетінің параметрлерін өзгерту, Басқару серверін құрылғыға жіберуге дайындалған кештегі пакет кескінін жаңартуға мәжбүрлейді.

Қашықтан орнату тапсырмасында құрылғыларды қайта жүктеуді басқару

Жиі қолданбаларды қашықтан орнатуды аяқтау үшін (әсіресе Windows платформасында) құрылғыны қайта іске қосу қажет.

Егер Kaspersky Security Center бағдарламаларды қашықтан орнату тапсырмасы қолданылса, жаңа тапсырма жасау шеберінде немесе жасалған тапсырма сипаттарының терезесінде (**Операциялық жүйені қайта іске қосу** бөлімі) Windows операциялық жүйесі бар құрылғыны қайта іске қосу қажеттілігінде әрекеттің нұсқасын таңдауға болады:

- **Құрылғыны қайта іске қоспау**. Бұл жағдайда автоматты қайта іске қосу орындалмайды. Орнатуды аяқтау үшін құрылғыны қайта іске қосу керек (мысалы, қолмен немесе құрылғыларды басқару тапсырмасы көмегімен). Қайта іске қосу қажеттілігі туралы ақпарат тапсырманы орындау нәтижелерінде және құрылғы күйінде сақталады. Бұл нұсқа серверлерге және үздіксіз жұмыс критикалық түрде маңызды басқа құрылғыларға орнату тапсырмалары үшін қолайлы.

- **Құрылғыны қайта іске қосу**. Бұл жағдайда, егер қайта іске қосу орнатуды аяқтау үшін қажет болса, қайта іске қосу автоматты түрде орындалады. Бұл нұсқа жұмыста мерзімді үзілістерге жол берілетін (сөндіру, қайта іске қосу) құрылғыларға арналған орнату тапсырмаларына қолайлы.

- **Пайдаланушыдан әрекетті орындауды сұрау**. Клиент құрылғысының экранында құрылғыны қолмен қайта жүктеу керек деген хабар пайда болады. Бұл нұсқа үшін қосымша параметрлерді конфигурациялауға болады: пайдаланушыға арналған хабар мәтіні, хабардың жиілігі, сондай-ақ қайта жүктеу мәжбүрлі түрде орындалатын уақыт (пайдаланушының растауынсыз). **Пайдаланушыдан әрекетті орындауды сұрау** нұсқасы пайдаланушылары қайта іске қосу үшін анағұрлым қолайлы сәтті таңдау мүмкіндігіне ие болуы тиіс жұмыс станцияларына анағұрлым қолайлы.

Антивирустық қолданбаның орнату пакетіндегі дерекқорларды жаңартудың орындылығы

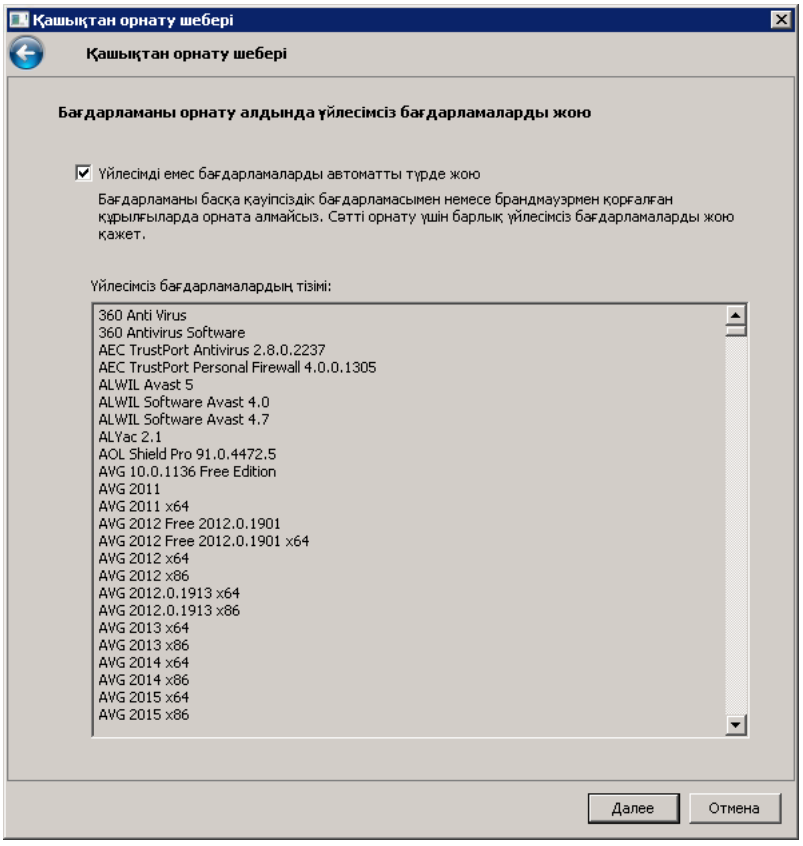
Орналастыру алдында, қауіпсіздік бағдарламасының дистрибутивімен бірге таратылатын антивирустық дерекқорларды (автопатч модульдерін қоса) жаңарту мүмкіндігін ескеру қажет. Орналастыруды бастамас бұрын қолданбаның орнату пакетінің құрамындағы дерекқорларды мәжбүрлеп жаңартқан жөн (мысалы, таңдалған орнату пакетінің мәнмәтіндік мәзіріндегі тиісті пәрменді қолдану арқылы). Бұл құрылғыларда қорғанысты орналастыруды аяқтау үшін қажет қайта жүктеу санын азайтады. Негізгі Серверден виртуалды Серверлерге ауыстырылған орнату пакеттерін қашықтан орнату үшін пайдаланған жағдайда, дерекқорларды тек негізгі Сервердегі бастапқы пакеттің өзінде жаңарту қажет. Бұл жағдайда, виртуалды Серверлерде ауыстырылған пакеттердегі дерекқорларды жаңартпаған жөн.

Үшінші тараптардың үйлесімсіз қауіпсіздік бағдарламаларын жою

Kaspersky қауіпсіздік бағдарламаларын Kaspersky Security Center құралдарымен орнату үшін, орнатылатын бағдарламамен үйлеспейтін үшінші тарап бағдарламалық жасақтамасын жою қажет болуы мүмкін. Бұл тапсырманы орындаудың екі негізгі тәсілі бар.

Орнату шебері көмегімен үйлесімсіз бағдарламаларды автоматты түрде жою

Орнату шеберін іске қосқан кезде, ол Kaspersky бағдарламасымен үйлесімсіз бағдарламалар тізімін көрсетеді:



Қашықтан орнату шеберінде көрсетілетін үйлесімсіз бағдарламалар тізімі

Kaspersky Security Center үйлесімсіз бағдарламалық жасақтаманы анықтайды. Тиісінше, сіз орнатуды жалғастыру үшін **Үйлесімді емес бағдарламаларды автоматты түрде жою** жалаушасын орната аласыз. Егер бұл жалаушаны алып тастаса және үйлесімсіз бағдарламалық жасақтаманы жоймаса, қате пайда болады және Kaspersky бағдарламасы орнатылады.

Үйлесімді емес бағдарламаларды автоматты түрде жоюға әртүрлі орнату түрлерімен қолдау көрсетіледі.

Үйлесімсіз бағдарламаларды бөлек тапсырма арқылы жою

Үйлесімсіз бағдарламаларды жою үшін *Бағдарламаны қашықтан жою* тапсырмасы қолданылады. Тапсырма қауіпсіздік бағдарламасын орнату тапсырмасынан бұрын, құрылғыларда іске қосылуы керек. Мысалы, орнату тапсырмасында **Басқа тапсырманы аяқтағанда** түріндегі кестені таңдауға болады, онда басқа тапсырма *Бағдарламаны қашықтан жою* тапсырмасы болып табылады.

Бұл жою тәсілі, қауіпсіздік бағдарламасы инсталляторы үйлесімсіз бағдарламалардың ешқайсысын сәтті жоя алмаған жағдайда қолданылғаны жөн.

Пәрмен желісі арқылы құпиясөзбен қорғалған Желілік агентті жою

Жою құпиясөзі орнатылған Желілік агент бағдарламасын қашықтан жою үшін пәрмен желісін пайдалануға болады.

Енді Kaspersky Security Center басқармайтын құпиясөзбен қорғалған құрылғыда орнатылған желілік агенттің құпиясөзін жоғалтып алсаңыз немесе ұмытып қалсаңыз, klmover утилитасын, Cleaner (cleaner.exe) құралын немесе пәрмен нұсқауын пайдаланып, бұл желілік агентті өшіре алмайсыз. Бұл жағдайда құпиясөзбен қорғалған желілік агент орнатылған құрылғыда операциялық жүйені қайта орнату қажет.

Желілік агентті пәрмен желісінен жою үшін:

1. Жою құпия сөзін он алтылық кодқа түрлендіріңіз.

   Құпиясөзді он алтылық кодқа түрлендіру үшін интернет-ресурсты, бағдарламалау ортасын, мәтіндік редакторды немесе басқа құралды пайдаланыңыз.

   Жасалған он алтылық кодты бөліктерге бөлу үшін пайдаланылатын шығыс бөлгішінің `00` мәніне орнатылғанын тексеріңіз. Мысалы, `51 77 65 72 74 79` он алтылық коды дұрыс емес, бірақ `5100770065007200740079 00` он алтылық коды дұрыс.

2. Пәрмен желісінде келесі пәрменді теріп, **ENTER** пернесін басыңыз:

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   Төмендегі кестеден желілік агентке арналған бағдарлама кодын таба аласыз.

Желілік агент бағдарламасының кодтары

Локализация тілі	Бағдарлама коды
Араб тілі	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
Болгар тілі	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
Чех тілі	{478A6A0B-D177-4402-B703-808C05C56B13}
Ағылшын тілі	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
Француз тілі	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
Неміс тілі	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
Венгр тілі	{8899A4D4-D678-49F8-AD96-0B784F58D355}
Итальян тілі	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
Жапон тілі	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
Кәріс тілі	{70812A40-973B-4DA1-96B9-C2011280CD99}
Поляк тілі	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
Португал тілі	{0F05E4E5-5A89-482C-9A62-47CC58643788}
Румын тілі	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
Орыс тілі	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
Жеңілдетілген қытай тілі	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
Испан тілі	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
Испан тілі (Мексика)	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}

Дәстүрлі қытай тілі	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
Түрік тілі	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Ерікті орындалатын файлдардың басқарылатын құрылғыларында іске қосу үшін Kaspersky Security Center қолданбаларын қашықтан орнату құралдарын қолдану

Орнату пакетін жасау шеберінің көмегімен, ерікті орындалатын файлды таңдауға және ол үшін пәрмен жолының параметрлерін белгілеуге болады. Бұл арада, орнату пакетіне таңдалған файлдың өзін де, осы файл орналасқан қалтаның барлығын да салып қоюға болады. Содан кейін, қашықтан орнату тапсырмасын жасап, жасалған орнату пакетін таңдау керек.

Тапсырманың жұмыс барысында, құрылғыларда жасау кезінде көрсетілген, пәрмен жолының параметрлері белгіленген орындалатын файл іске қосылады.

Microsoft Windows Installer (MSI) пішіміндегі инсталляторлар қолданылса, Kaspersky Security Center бағдарламасы орнату нәтижесін талдау бойынша штаттық мүмкіндіктерді қолданады.

Осалдықтар мен патчтарды басқаруға арналған лицензия, корпоративтік ортада кеңінен таралған қолдау көрсетілетін қолданбалардың бірі үшін орнату пакетін жасау кезінде, Kaspersky Security Center бағдарламасы өзінің жаңартылатын дерекқорындағы орнату нәтижелерін талдау және орнату ережелерін де қолданады.

Өзге жағдайларда, орындалатын файлдар үшін әдепкі бойынша іске қосылған процестің және ол іске қосқан еншілес процестердің барлығының аяқталғанын күту керек. Іске қосылған процестер аяқталған кезде, тапсырма бастапқы процесті қайтару кодына қарамастан сәтті аяқталады. Тапсырманың осындай жүріс-тұрысын өзгерту үшін, тапсырманың жасау алдында, жасалған орнату пакетінің қалтасы мен оның ішкі қалталарында Kaspersky Security Center жасаған kpd кеңейтімі бар файлдарды қолмен өзгерту керек.

.kpd файлдары ASCII кодтауын пайдаланады. .kud файлдары Юникод кодтауын пайдаланады.

Тапсырма іске қосылған процестің аяқталуын күтпеуі үшін, [SetupProcessResult] секциясында Wait параметрі үшін 0 мәнін белгілеу керек:

```
[SetupProcessResult]
Wait=0
```

Windows платформасында тапсырма өзі іске қосқан еншілес процестердің емес, бастапқы процестің аяқталуын ғана күтуі үшін, онда [SetupProcessResult] секциясында WaitJob параметрі үшін 0 мәнін белгілеу керек, мысалы:

```
[SetupProcessResult]
WaitJob=0
```

Жүріп жатқан процестің қайтару кодына байланысты тапсырма сәтті аяқталуы немесе қате көрсетілуі үшін, қате кодын файлға сақтайтын орындалатын .bat файлын жасаңыз, мысалы:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Содан кейін жаңадан жасалған орнату пакеті қалтасында Kaspersky Security Center жасаған .kud файлдарын өзгертіңіз:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

Бұл жағдайда, атап көрсетілгендерден ерекшеленетін кез келген код қатені білдіреді.

Тапсырманың нәтижелерінде тапсырманың сәтті аяқталғаны туралы түсініктемесі жазылған жол немесе қателер туралы хабар көрсетілуі үшін, [SetupProcessResult_SuccessCodes] және [SetupProcessResult_ErrorCodes] секцияларында процесті қайтару кодтарына сай келетін қателердің қысқаша сипаттамаларын белгілеу керек, мысалы:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

Kaspersky Security Center бағдарламасының құрылғыны қайта іске қосуды басқару бойынша құралдарын қолдану үшін (қайта іске қосу операцияны аяқтау үшін керек болса), онда [SetupProcessResult_NeedReboot] секциясында қайта іске қосу қажеттілігін білдіретін процесті қайтару кодтарын қосымша түрде атап көрсету керек:

```
[SetupProcessResult_NeedReboot]
3010=
```

Орналастыру мониторингі

Kaspersky Security Center орналастыруды бақылау, сондай-ақ басқарылатын құрылғыларда қауіпсіздік бағдарламасы мен Желілік агенттің болуын бақылау үшін **Орналастыру** блогындағы түрлі-түсті индикаторға назар аудару керек. Индикатор Басқару консолінің негізгі терезесіндегі Басқару сервері түйінің жұмыс аймағында орналасқан. Индикатор орналастырудың ағымдағы күйін көрсетеді. Индикатордың жанында Желілік агенттері мен қауіпсіздік бағдарламалары орнатылған құрылғылар саны көрсетіледі. Белсенді орнату тапсырмалары болған кезде, тапсырмаларды орнату прогресі көрсетіледі. Орнату қателері болған кезде, мұнда қателердің саны көрсетіледі. Қате туралы егжей-тегжейлі ақпаратты сілтеме арқылы қарап шығуға болады.

Сонымен қатар, **Топтар** қойыншасында **Басқарылатын құрылғылар** қалтасының жұмыс аймағын орналастыру диаграммасын пайдалануға болады. Диаграмма орналастыру процесін көрсетеді: Желілік агенті жоқ, Желілік агенті бар, Желілік агенті пен қауіпсіздік бағдарламасы бар құрылғылардың саны.

Орналастыру барысының (немесе нақты орнату тапсырмасының) барынша егжей-тегжейлі сипаттамасын тиісті қашықтан орнату тапсырмасын орындау нәтижелері терезесінде көруге болады: Тапсырманың мәнмәтіндік мәзірінен **Нәтижелер** тармағын таңдаңыз. Терезеде екі тізім көрсетіледі: жоғарғы тізімде құрылғылардағы тапсырма күйлерінің тізімі, ал төменгі тізімде – қазіргі уақытта жоғарғы тізімде таңдалған құрылғыдағы тапсырма оқиғаларының тізімі бар.

Орналастыру кезіндегі қателер туралы ақпарат Басқару серверінің Kaspersky Event журналына жазылады. Қателер туралы ақпарат **Есептер мен хабарландырулар** қалтасының **Оқиғалар** ішкі қалтасындағы тиісті оқиғаларды таңдауда да қолжетімді.

Инсталляторлар параметрлерін конфигурациялау

Бөлім Kaspersky Security Center инсталляторлар файлдары және орнату параметрлері туралы ақпаратты, сондай-ақ басқару серверін және желілік агентті "тыныш" режимде орнату жөніндегі ұсынымдарды қамтиды.

Жалпы ақпарат

Kaspersky Security Center 15.1 құрамдастары – Басқару сервері, Желілік агент, Басқару консолінің инсталляторлары Windows Installer технологиясына негізделген. Инсталлятордың өзегі – MSI пакеті болып саналады. Дистрибутив қаптамасының осындай пішімі Windows Installer технологиясының барлық артықшылықтарын қолдануға мүмкіндік береді: масштабталу, патчтау жүйесін, түрлендіру жүйесін қолдану мүмкіндігі, үшінші тарап шешімдерімен орталықтандырылған түрде орнату мүмкіндігі, операциялық жүйеде тіркелу айқындығы.

Тыныш режимде орнату (жауаптар файлымен)

Басқару сервері мен Желілік агенттің инсталляторларында, пайдаланушының қатысуынсыз тыныш режимде орнатуға арналған параметрлер жазылған жауаптар файлымен (ss_install.xml) жұмыс істеу мүмкіндігі іске асырылған. ss_install.xml файлы MSI пакетімен бір қалтада орналасқан және тыныш режимде орнату кезінде автоматты түрде қолданылады. Сіз "/s" пәрмен жолының кілті арқылы автоматты түрде орнату режимін қоса аласыз.

Іске қосу мысалы:

```
setup.exe /s
```

Орнатушы бағдарламасын тыныш режимде іске қоспас бұрын, Лицензиялық келісімді оқып шығыңыз. Kaspersky Security Center дистрибутиві құрамына Лицензиялық келісім мәтіні бар TXT файлы кірмесе, бұл файлды Kaspersky сайтынан жүктеп алуға болады.

ss_install.xml файлы Kaspersky Security Center инсталляторы параметрлерінің ішкі пішімі болып табылады. Дистрибутивтер құрамында әдепкі бойынша параметрлері бар ss_install.xml файлы жеткізіледі.

ss_install.xml файлын қолмен өзгертудің қажеті жоқ. Бұл файл, Басқару консолiндегі орнату пакеттерінің параметрлерін өзгерту кезінде Kaspersky Security Center құралдарымен өзгертіледі.

Басқару серверін орнату үшін жауап файлын өзгерту үшін:

1. Kaspersky Security Center дистрибутивін ашыңыз. EXE файлының толық пакетін қолдансаңыз, оны мұрағаттан шығарыңыз.

2. Сервер қалтасын қалыптастырыңыз, пәрмен жолын ашыңыз және келесі пәрменді орындаңыз:

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center орнату бағдарламасы іске қосылады.

3. Kaspersky Security Center орнатуды конфигурациялау үшін шебердің нұсқауларын орындаңыз.

Шебердің жұмысы аяқталғаннан кейін, жауаптар файлы сіз көрсеткен жаңа параметрлерге сай автоматты түрде өзгертіледі.

Желілік агентті тыныш режимде орнату (жауаптар файлы жоқ)

Желілік агент, MSI сипаттарының мәндерін стандартты түрде белгілей отырып, тек бір msi пакетінің көмегімен орнатылуы мүмкін. Мұндай сценарий топтық саясатты қолдана отырып, Желілік агентті орнатуға мүмкіндік береді.

Kaspersky Network Agent.msi орнату пакетінің атын өзгертпеңіз. Пакет атауы өзгертілсе, желілік агентті жаңартқан кезде орнату қателері пайда болуы мүмкін.

MSI сипаттары арқылы берілген параметрлер мен жауап файлында берілген параметрлер арасында қайшылық болмас үшін `DONT_USE_ANSWER_FILE=1` сипатын белгілеу арқылы жауап файлын өшіру мүмкіндігі қарастырылған. MSI файлы Kaspersky Security Center бағдарламасының дистрибутивінде Packages\NetAgent\exec қалтасында орналасқан. Төменде msi пакетін пайдаланып Желілік агент инсталляторын іске қосудың мысалы келтірілген.

Желілік агентті интерактивті емес режимде орнату Лицензиялық келісімді қабылдауды талап етеді. `EULA=1` параметрін тек Лицензиялық келісімнің шарттарын толық оқып, түсініп, қабылдаған жағдайда ғана қолданыңыз.

Мысалы:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Сондай-ақ, түрлендіру файлын (mst кеңейтімі бар файл) алдын ала дайындау арқылы msi пакетін орнату параметрлерін белгілеуге болады. Пәрмен келесідей болады:

Мысалы:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Бір пәрменде бірнеше түрлендіру файлын көрсетуге болады.

Windows Installer көмегімен желі агентін жаңартқыңыз келсе, келесі пәрменді орындаңыз:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

setup.exe арқылы орнату параметрлерін ішінара конфигурациялау

setup.exe арқылы бағдарламаларды орнатуды іске қосу арқылы кез келген MSI сипаттарының мәндерін MSI пакетіне жіберуге болады.

Пәрмен келесідей болады:

Мысалы:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Басқару серверін орнату параметрлері

Төмендегі кестеде, Басқару серверін орнату кезінде конфигурациялауға болатын MSI сипаттары сипатталған. EULA және PRIVACYPOLICY қоспағанда, барлық параметрлер міндетті емес.

Басқару серверін тыныш режимде орнату параметрлері

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
EULA	Лицензиялық келісімнің шарттарымен келісу (міндетті параметр)	• 1 – Мен Лицензиялық келісімді толығымен оқып шыққанымды және оның шарттарын қабылдайтынымды растаймын. • Басқа мән немесе белгіленбеген – Лицензиялық келісімнің шарттарымен келіспейсіз (орнату жүзеге асырылмайды).
PRIVACYPOLICY	Құпиялық саясатының шарттарымен келісу (міндетті параметр)	• 1 – Менің деректерім Құпиялылық саясатында сипатталғандай өңделетінін және тасымалданатынын (соның ішінде үшінші тараптарға) білемін және оған келісемін. Құпиялылық саясатын толықтай оқып, түсінгенімді растаймын. • Басқа мән немесе белгіленбеген – Мен Құпиялылық саясатының шарттарын қабылдамаймын (орнату орындалмайды).
INSTALLATIONMODETYPE	Басқару серверін орнату түрі	• Стандартты. • Таңдаулы.
INSTALLDIR	Бағдарламаны орнату қалтасы	Жол мәні.
ADDLOCAL	Орнату үшін құрамдастар тізімі (үтір арқылы)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Басқару серверін дұрыс орнату үшін жеткілікті құрамдастардың минималды тізімі: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Желінің өлшемі	• NRT_1_100 – 1-ден 100 құрылғыға дейін. • NRT_100_1000 – 101-ден 1000 құрылғыға дейін. • NRT_GREATER_1000 – 1000-нан астам құрылғы.
SRV_ACCOUNT_TYPE	Басқару сервері қызметінің жұмыс істеуі үшін пайдаланушыны белгілеу тәсілі	• SrvAccountDefault – пайдаланушы есептік жазбасы автоматты түрде жасалады. • SrvAccountUser – пайдаланушы есептік жазбасы қолмен белгіленген.
SERVERACCOUNTNAME	Қызметке арналған пайдаланушы атауы	Жол мәні.
SERVERACCOUNTPWD	Қызмет үшін пайдаланушы құпиясөзі	Жол мәні.
DBTYPE	Дерекқор түрі	• MySQL – MySQL немесе MariaDB дерекқоры қолданылады. • MSSQL – Microsoft SQL Server (SQL Express) дерекқоры қолданылады.
MYSQLSERVERNAME	MySQL немесе MariaDB серверінің толық атауы	Жол мәні.
MYSQLSERVERPORT	MySQL немесе MariaDB серверіне қосылуға арналған порт нөмірі	Сандық мән.
MYSQLDBNAME	MySQL немесе MariaDB сервері дерекқорының атауы	Жол мәні.
MYSQLACCOUNTNAME	MySQL немесе MariaDB серверінің дерекқорына қосуға арналған пайдаланушы атауы	Жол мәні.

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
MYSQLACCOUNTPWD	MySQL немесе MariaDB серверінің дерекқорына қосуға арналған пайдаланушы құпиясөзі	Жол мәні.
MSSQLCONNECTIONTYPE	MSSQL дерекқорын қолдану түрі	• InstallMSSEE – пакеттен орнату. • ChooseExisting – орнатылған серверді қолдану.
MSSQLSERVERNAME	SQL Server үлгісінің толық атауы	Жол мәні.
MSSQLDBNAME	SQL Server дерекқорының атауы	Жол мәні.
MSSQLAUTHTYPE	SQL Server серверіне қосылу кезіндегі түпнұсқалық растама тәсілі	• Windows. • SQLServer.
MSSQLACCOUNTNAME	SQL Server серверіне SQLServer режимінде қосылу үшін пайдаланушы атауы	Жол мәні.
MSSQLACCOUNTPWD	SQL Server серверіне SQLServer режимінде қосылу үшін пайдаланушы құпиясөзі	Жол мәні.
CREATE_SHARE_TYPE	Ортақ қатынасы бар қалтаны белгілеу тәсілі	• Create – ортақ қатынасы бар жаңа қалтаны жасау. Бұл жағдайда, келесі сипаттар белгіленуі тиіс: • SHARELOCALPATH – жергілікті қалтаға апаратын жол. • SHAREFOLDERNAME – қалтаның желілік атауы. • Бос – EXISTSHAREFOLDERNAME сипаты белгіленуі тиіс.
EXISTSHAREFOLDERNAME	Қолданыстағы ортақ қатынасы бар қалтаға апаратын толық жол	Жол мәні.
SERVERPORT	Басқару серверіне қосылуға арналған порт нөмірі	Сандық мән.
SERVERSSLPORT	Басқару серверімен SSL қосылымын орнатуға арналған порт нөмірі	Сандық мән.
SERVERADDRESS	Басқару сервері мекенжайы	Жол мәні.
SERVERCERT2048BITS	Басқару серверінің сертификатына арналған кілттің ұзындығы (бит түрінде)	• 1 – Басқару серверінің сертификатына арналған кілттің ұзындығы 2048 битті құрайды. • 0 – Басқару серверінің сертификатына арналған кілттің ұзындығы 1024 битті құрайды. • Егер параметр белгіленбесе, онда Басқару серверінің сертификатына арналған кілттің ұзындығы 2048 битті құрайды.
MOBILESERVERADDRESS	Ұялы құрылғылар қосылатын Басқару серверінің мекенжайы; MobileSupport құрамдасы таңдалмаса, еленбейді	Жол мәні.

Желілік агентті орнату параметрлері

Төмендегі кестеде, Желілік агентті орнату кезінде конфигурациялауға болатын MSI сипаттары сипатталған. SERVERADDRESS қоспағанда, барлық параметрлер міндетті емес.

MSI сипаттары

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
DONT_USE_ANSWER_FILE	Жауап файлынан орнату параметрлерін оқу.	• 1 • Мәні жоқ
INSTALLDIR	Орнату қалтасы.	
SERVERADDRESS	Басқару серверінің мекенжайы (міндетті параметр).	
SERVERPORT	Басқару серверіне қосылу портының нөмірі.	

MSI сипаты	Сипаттамасы	Қолжетімді мәндері
SERVERSSLPORT	SSL қосылымына арналған порт нөмірі.	
USESSL	SSL байланысын пайдалану керек пе.	• 1 • Мәні жоқ
OPENUDPPORT	UDP портын ашу керек пе.	• 1 • Мәні жоқ
UDPPORT	UDP портының нөмірі.	
USEPROXY	Прокси-серверді пайдалану керек пе.	• 1 • Мәні жоқ
PROXYADDRESS	Прокси серверінің мекенжайы.	
PROXYPORT	Басқару серверіне қосылу портының нөмірі.	
PROXYLOGIN	Прокси-серверге қосылуға арналған есептік жазба.	
PROXYPASSWORD	Прокси-серверге қосылуға арналған есептік жазба құпиясөзі. Орнату пакеттерінің параметрлерінде артықшылықты есептік жазбалардың деректерін көрсетпеңіз.	
GATEWAYMODE	Қосылым шлюзін пайдалану режимі.	• 0 – қосылымдар шлюзін пайдаланбау; • 1 – бұл Желілік агентті қосылым шлюзі ретінде пайдалану; • 2 – Басқару серверіне қосылым шлюзі арқылы қосылу.
GATEWAYADDRESS	Қосылым шлюзі мекенжайы.	
CERTSELECTION	Сертификат алу тәсілі.	• GetOnFirstConnection – Басқару серверінен сертификат алу; • GetExistent – бұрыннан бар сертификатты таңдау. Егер бұл нұсқа таңдалса, CERTFILE сипаты көрсетілуі керек.
CERTFILE	Сертификат файлының жолы.	
VMVDI	Enable dynamic mode for VDI	• 1 • Мәні жоқ
LAUNCHPROGRAM	Желілік агент қызметін орнатқаннан кейін іске қосу керек пе.	• 1 • Мәні жоқ

Виртуалды инфрақұрылым

Kaspersky Security Center бағдарламасы виртуалды машиналармен жұмыс істеуді қолдайды. Сіз әр виртуалды машинада Желілік агент пен қауіпсіздік бағдарламаларын орната аласыз, сонымен қатар виртуалды машиналарды гипервизор деңгейінде қорғай аласыз. Бірінші жағдайда, виртуалды машиналарды қорғау үшін қарапайым қауіпсіздік бағдарламасын да, Kaspersky Security for Virtualization Light Agent бағдарламасын да қолдануға болады. Екінші жағдайда, Kaspersky Security for Virtualization Agentless бағдарламасын қолдана аласыз.

Kaspersky Security Center бағдарламасы виртуалды машиналарды алдыңғы күйге шегіндіру мүмкіндігін қолдайды.

Виртуалды машиналарға түсетін жүктемені азайту бойынша ұсынымдар

Желілік агентті виртуалды машинаға орнатқан жағдайда, виртуалды машиналар үшін өте пайдалы емес Kaspersky Security Center функционалдығының бір бөлігін өшіру туралы ойлану керек.

Желілік агентті виртуалды машинаға немесе болашақта виртуалды машиналар алынатын үлгіге орнатқан кезде келесі әрекеттерді орындау ұсынылады:

- қашықтан орнату орындалып жатса, Желілік агенттің орнату пакетінің сипаттар терезесінде (**Кеңейтілген** бөлімінде) **VDI параметрлерін оңтайландыру** параметрін таңдаңыз;
- егер шебердің көмегімен интерактивті орнату орындалып жатса, шебер терезесінде **Виртуалды инфрақұрылым үшін Желілік агент параметрлерін оңтайландыру** параметрін таңдаңыз.

Параметрлерді таңдау, Желілік агенттің параметрлерін, әдепкі бойынша (саясатты қолданар алдында) келесі функциялар өшірілетіндей етіп өзгертеді:

- Орнатылған бағдарламалық жасақтама туралы ақпарат алу
- Аппараттық жасақтама туралы ақпарат алу
- Осалдықтардың болуы туралы ақпарат алу
- Қажетті жаңартулар туралы ақпарат алу

Әдетте, аталған функциялар виртуалды машиналарда қажет емес, өйткені олардағы бағдарламалық жасақтама мен виртуалды аппараттық жасақтама біркелкі.

Функцияларды өшіру қайтымды. Егер өшірулі функциялардың кез келгені қажет болса, оны Желілік агент саясаты немесе Желілік агенттің жергілікті параметрлері арқылы қосуға болады. Желілік агенттің жергілікті параметрлері Басқару консоліндегі тиісті құрылғының контекстік мәзірінен қолжетімді.

Динамикалық виртуалды машиналарды қолдау

Kaspersky Security Center динамикалық виртуалды машиналарды қолдайды. Егер ұйымның желісінде виртуалды инфрақұрылым орналастырылған болса, онда кейбір жағдайларда динамикалық (уақытша) виртуалды машиналар қолданылуы мүмкін. Мұндай машиналар, әкімші алдын ала дайындаған үлгіден ерекше атаулармен жасалады. Пайдаланушы жасалған машинамен біраз уақыт жұмыс істейді, ал виртуалды машина өшірілгеннен кейін виртуалды инфрақұрылымнан жойылады. Егер ұйымның желісінде Kaspersky Security Center орналастырылған болса, оған орнатылған Желілік агенті бар виртуалды машина Басқару серверінің дерекқорына қосылады. Виртуалды машинаны өшіргеннен кейін, ол туралы жазба Басқару сервері дерекқорынан да жойылуы керек.

Виртуалды машина жазбаларын автоматты түрде жою функционалдығы жұмыс істеуі үшін Желілік агентті динамикалық виртуалды машиналар жасалатын үлгіе орнатқан кезде **VDI үшін динамикалық режимді қосу** параметрін таңдау керек:

- қашықтан орнату жағдайында – Желілік агенттің орнату пакетінің сипаттары терезесінде (**Кеңейтілген бөлімі**);
- интерактивті орнату жағдайында – Желілік агентті орнату шеберінде.

VDI үшін динамикалық режимді қосу параметрі Желілік агентті физикалық құрылғыларға орнатқан кезде таңдалмауы керек.

Машиналар жойылғаннан кейін Динамикалық виртуалды машиналардағы оқиғалар біраз уақыт бойы Басқару серверінде сақталуы керек болса, онда Басқару сервері сипаттары терезесінде, **Оқиғалар қоймасы** бөлімінде **Құрылғылар жойылғаннан кейін оқиғаларды сақтау** параметрін таңдап, күндердегі оқиғаларды сақтаудың ең ұзақ уақытын көрсету керек.

Динамикалық виртуалды машиналарда дискіні шифрлауды қосуға кеңес бермейміз.

Виртуалды машиналарды көшіруді қолдау

Виртуалды машинаны орнатылған Желілік агентімен бірге көшіру немесе оны орнатылған Желілік агентпен бірге үлгіден жасау – қатты дискінің кескінін түсіру және көшіру арқылы Желілік агенттерді орналастыруға тең келеді. Сондықтан, жалпы жағдайда, виртуалды машиналарды көшіру кезінде диск кескінін көшіру арқылы орналастыру сияқты әрекеттерді орындау қажет.

Алайда, төменде сипатталған екі жағдайда Желілік агент көшіру фактісін автоматты түрде анықтайды. Сондықтан, "Құрылғының қатты дискісін түсіру және көшіру" бөлімінде сипатталған күрделі әрекеттерді орындау міндетті емес:

- Желілік агентті орнату кезінде **VDI үшін динамикалық режимді қосу** параметрі таңдалды: операциялық жүйені әрбір рет қайта іске қосқаннан кейін мұндай виртуалды машина, оны көшіру фактісіне қарамастан, жаңа құрылғы болып саналатын болады.
- Келесі гипервизорлардың бірі қолданылады: VMware™, HyperV® немесе Xen®: Желілік агент виртуалды машинаны көшіру фактісін виртуалды аппараттық жасақтаманың өзгерген идентификаторлар бойынша анықтайды.

Виртуалды аппараттық жасақтаманың өзгерістерін талдау мүлдем сенімді емес. Бұл әдісті кеңінен қолданбас бұрын, оның жұмысқа жарамдылығын ұйымда қолданылатын гипервизордың нұсқасы үшін аздаған виртуалды машиналарда алдын ала тексеріп алу керек.

Желілік агенті бар құрылғылар үшін файлдық жүйені шегіндіруді қолдау

Kaspersky Security Center бағдарламасы таратылған бағдарлама болып саналады. Желілік агенті орнатылған құрылғылардың бірінде файлдық жүйені алдыңғы күйге шегіндіру деректерді синхрондамауға және Kaspersky Security Center дұрыс жұмыс істемеуіне әкеледі.

Файлдық жүйені (немесе оның бір бөлігін) алдыңғы күйге шегіндіру келесі жағдайларда болуы мүмкін:

- қатты дискінің кескінін көшіру кезінде;
- виртуалды инфрақұрылым арқылы виртуалды машинаның күйін қалпына келтіру кезінде;
- сақтық көшірмеден немесе қалпына келтіру нүктесінен деректерді қалпына келтіру кезінде.

Kaspersky Security Center үшін, Желілік агенті орнатылған құрылғылардағы үшінші тарап бағдарламалық жасақтамасы %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ қалтасына әсер ететін сценарийлер ғана маңызды. Сондықтан, мүмкіндік болса, бұл қалтаны қалпына келтіру процедурасынан әрқашан алып тастап отыру керек.

Бірқатар ұйымдарда жұмыс регламенті құрылғылардың файлдық жүйесінің күйін шегіндіруді көздейтіндіктен, Kaspersky Security Center бағдарламасында, 10 Maintenance Release 1 нұсқасынан бастап (Басқару сервері мен Желілік агенттер нұсқасы 10 Maintenance Release 1 немесе одан жоғары болуы керек), Желілік агенті орнатылған құрылғыларда файлдық жүйенің шегіндірілуін анықтауды қолдау мүмкіндігі қосылды. Табылған жағдайда, мұндай құрылғылар деректерді толық тазалаумен және толық синхрондаумен бірге Басқару серверіне автоматты түрде қайта қосылады.

Kaspersky Security Center 15.1 нұсқасында файлдық жүйенің шегіндірілуін анықтауды қолдау әдепкі бойынша қосылады.

Кез келген мүмкіндік туындаған кезде, %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ қалтасын Желілік агенті орнатылған құрылғыларға шегіндіруден аулақ болу керек, өйткені деректерді толық қайта синхрондау көп ресурстарды қажет етеді.

Басқару сервері орнатылған құрылғы үшін жүйенің күйін шегіндіруге жол берілмейді. Басқару сервері пайдаланатын дерекқордың алдыңғы күйіне шегіндіру де қолайсыз.

Сақтық көшірмеден Басқару серверінің күйін тек штаттық klbackup утилитасын пайдаланып қалпына келтіруге болады.

Автономды пайдаланушыларға арналған қосылым профильдері туралы

Ноутбуктерді (бұдан әрі - "құрылғылар") пайдаланатын автономды пайдаланушылар жұмыс істеген кезде, құрылғының желідегі ағымдағы жайғасымына байланысты Басқару серверіне қосылу тәсілін өзгерту немесе Басқару серверлері арасында ауысу қажет болуы мүмкін.

Қосылым профильдеріне тек Windows және macOS басқаратын құрылғылар үшін ғана қолдау көрсетіледі.

Бір Басқару серверінің әртүрлі мекенжайларын пайдалану

Желілік агенті орнатылған құрылғылар әртүрлі уақыт аралығында ұйымның ішкі желісінен де, интернеттен де Басқару серверіне де қосыла алады. Бұл жағдайда, Желілік агент Басқару серверіне қосылу үшін әртүрлі мекенжайларды қолдануы қажет болуы мүмкін: интернеттен қосылған кезде Сервердің сыртқы мекенжайы және ішкі желіден қосылған кезде Сервердің ішкі мекенжайы.

Бұл үшін, Желілік агент саясатының сипаттарында интернеттен Басқару серверіне қосылу үшін профиль қосыңыз. Саясат сипаттары, **Байланыстардың профильдері** салынған бөлімінде профильді қосыңыз (**Қосылымдар** бөлімі). Профиль жасау терезесінде **Тек жаңартуларды алу үшін пайдалану** параметрін өшіріп, **Қосылым параметрлерін осы профильде көрсетілген Басқару серверінің параметрлерімен синхрондау** параметрін таңдау керек. Егер қосылым шлюзі Басқару серверіне қатынасу үшін пайдаланылса (мысалы, Интернеттен қатынасу: Желілік агент демилитаризацияланған аймақтағы қосылым шлюзі ретінде бөлімінде сипатталған Kaspersky Security Center конфигурациясында), қосылым профилінде тиісті өрістегі қосылым шлюзінің мекенжайы көрсетілуі керек.

Ағымдағы желіге байланысты Басқару серверлері арасында ауысу

Егер ұйымда әртүрлі Басқару серверлері бар бірнеше кеңселер болса және олардың арасында Желілік агенті орнатылған құрылғылардың бір бөлігі жылжытылса, онда Желілік агент құрылғы орналасқан кеңсенің жергілікті желісін Басқару серверіне қосылуы керек.

Бұл жағдайда, Желілік агент саясатының сипаттарында бастапқы үйдегі Басқару сервері орналасқан үйдегі кеңсені қоспағанда, әрбір кеңсе үшін Басқару серверіне қосылу профилін жасау керек. Байланыс профильдерінде тиісті Басқару серверлерінің мекенжайларын көрсетіп, **Тек жаңартуларды алу үшін пайдалану** параметрін таңдаңыз немесе өшіріңіз:

- Желілік агент үйдегі Басқару серверімен синхрондауды қажет етсе, ал жергілікті Сервер тек жаңартуларды жүктеу үшін пайдаланылса, параметрді таңдаңыз;
- Желілік агент жергілікті Басқару сервері тарапынан толығымен басқарылуы қажет болса, параметрді өшіріңіз.

Әрі қарай, сіз жасалған профильдерге ауысу шарттарын конфигурациялауыңыз керек: "үйдегі кеңсені" қоспағанда, кеңселердің әрқайсысы үшін кемінде бір шарт. Мұндай шарттардың әрқайсысының мәні кеңселердің біріне тән бөлшектерді желілік ортада табуға негізделеді. Егер шарт шындыққа айналса, тиісті профиль белсендіріледі. Егер шарттардың ешқайсысы дұрыс болмаса, Желілік агент үйдегі Басқару серверіне ауысады.

Ұялы құрылғыларды қолдауды орналастыру

Бұл бөлімде ұялы құрылғыларды басқару функциясының бастапқы орналастырылуы туралы ақпарат берілген.

KES құрылғыларын Басқару серверіне қосу

Құрылғыларды Басқару серверіне қосу тәсіліне байланысты, KES құрылғылары үшін Kaspersky Device Management for iOS орналастырудың екі схемасы бар:

- Басқару серверіне құрылғыларды тікелей қосу арқылы орналастыру схемасы;
- Kerberos Constrained Delegation қолдайтын кері прокси-серверді қолданатын орналастыру диаграммасы.

Құрылғыларды Басқару серверіне тікелей қосу

KES құрылғылары Басқару серверінің 13292 портына тікелей қосыла алады.

Түпнұсқалық растама тәсіліне байланысты, KES құрылғыларын Басқару серверіне қосудың екі нұсқасы бар:

- Пайдаланушы сертификатын қолдану арқылы құрылғыларды қосу
- Пайдалану сертификатынсыз құрылғыларды қосу

Пайдаланушы сертификатын қолдану арқылы құрылғыны қосу

Пайдаланушы сертификатын қолдану арқылы құрылғыны қосу кезінде, осы құрылғы Басқару серверінің құралдарымен тиісті сертификат тағайындалған пайдаланушының есептік жазбасына байланады.

Бұл жағдайда, екі жақты SSL түпнұсқалық растамасы (mutual authentication) қолданылады. Басқару сервері де, құрылғы да сертификаттардың көмегімен түпнұсқалық растамадан өткізіледі.

Пайдалану сертификатынсыз құрылғыны қосу

Пайдаланушы сертификатынсыз құрылғыны қосу кезінде, ол Басқару серверіндегі ешбір пайдаланушы есептік жазбасына байланбайды. Бірақ құрылғы кез келген сертификатты алған кезде, бұл құрылғы Басқару серверінің құралдарымен тиісті сертификат тағайындалған пайдаланушыға байланады.

Құрылғыны Басқару серверіне қосу кезінде бір жақты SSL түпнұсқалық растамасы (one-way SSL authentication) қолданылып, Басқару сервері сертификаттың көмегімен түпнұсқалық растамадан өтеді. Құрылғы пайдаланушы сертификатын алған кезде, түпнұсқалық растама түрі екі жақты SSL түпнұсқалық растамасына (2-way SSL authentication, mutual authentication) өзгертіледі.

Kerberos (KCD) мәжбүрлеп табыстау арқылы KES құрылғыларын Серверге қосу схемасы

KES құрылғыларын Kerberos Constrained Delegation (KCD) көмегімен Басқару серверіне қосу схемасы мыналарды қамтиды:

- KCD қолдайтын кері прокси-сервермен интеграция;
- ұялы құрылғылардың түпнұсқалық растамасы үшін Kerberos Constrained Delegation (бұдан әрі KCD) мәжбүрлеп табыстауын пайдалану;
- пайдаланушы сертификаттарын пайдалану үшін жалпыға ортақ кілттер инфрақұрылымымен (Public Key Infrastructure, бұдан әрі PKI) біріктіру.

Осы қосылым схемасын пайдалану кезінде мыналарды ескеру қажет:

- KES құрылғыларын кері прокси-серверге қосылым түрі "two-way SSL authentication" болуы тиіс, яғни құрылғы кері прокси-серверге өзінің пайдаланушы сертификаты арқылы қосылуы керек. Бұл үшін құрылғыда орнатылған Kaspersky Endpoint Security for Android орнату пакетіне пайдаланушы сертификатын кіріктіру қажет. Бұл KES пакетін осы құрылғы (пайдаланушы) үшін арнайы Басқару сервері жасауы керек.
- Мобильді протокол үшін әдепкі бойынша серверлік сертификаттың орнына арнайы (кастомизацияланған) сертификат көрсетілуі керек:

  1. Басқару сервері сипаттары терезесінде, **Параметрлер** бөлімінде **Ұялы құрылғыларға арналған портты ашу** жалаушасын қою және ашылмалы тізімнен **Сертификат қосу** тармағын таңдау.
  2. Ашылған терезеде, Басқару серверінде мобильді протоколға қатынасу нүктесін жариялау кезінде кері прокси-серверде берілген дәл сол сертификатты көрсетіңіз.

- KES құрылғылары үшін пайдаланушы сертификаттарын домендік Certificate Authority (CA) шығаруы керек. Доменде бірнеше түбірлік CA болса, онда пайдаланушы сертификаттары кері прокси-серверге арналған жарияланымда жазылған CA тарапынан шығарылуы тиіс.

Пайдаланушы сертификатының жоғарыда айтылған талапқа сәйкестігі бірнеше тәсілмен қамтамасыз етілуі мүмкін:

- Орнату пакеттерін жасау шеберінде және сертификаттарды орнату шеберінде арнайы пайдаланушы сертификатын көрсету.
- Басқару серверін домендік PKI инфрақұрылымымен біріктіру және сертификаттарды шығару ережелерінде тиісті параметрді конфигурациялау:
  1. **Мобильді құрылғыларды басқару** қалтасындағы консоль шежіресінен **Сертификаттар** салынған қалтасын таңдаңыз.
  2. **Сертификаттар** қалтасының жұмыс аймағында, **Сертификат беру ережелерін конфигурациялау** түймесі арқылы **Сертификаттарды шығару ережелері** терезесін ашыңыз.
  3. **PKI жүйесімен интеграциялау** бөлімінде жалпыға ортақ кілт инфрақұрылымымен біріктіруді конфигурациялаңыз.
  4. **Ұялы құрылғы сертификаттарын шығару** бөлімінде сертификаттар көзін көрсетіңіз.

Келесі болжамдармен KCD шектеулі табыстау конфигурациясы мысалын қарастырайық:

- Басқару серверінде мобильді протоколға қатынасу нүктесі 13292-портта көтерілген;
- кері прокси-серверден құрылғы атауы – firewall.mydom.local;
- Басқару сервері бар құрылғының атауы – ksc.mydom.local;
- Мобильді протоколға қатынасу нүктесін сырты жариялау атауы – kes4mob.mydom.global.

Басқару сервері үшін домендік есептік жазба

Басқару сервері қызметі жұмыс істейтін домендік есептік жазбаны (мысалы, KSCMobileSrvcUsr) жасау қажет. Басқару сервері қызметі үшін есептік жазбаны, Басқару серверін орнату кезінде немесе klsrvswch утилитасын пайдалану арқылы көрсетуге болады. klsrvswch утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Домендік есептік жазбаны келесі себептерге байланысты көрсету қажет:

- KES құрылғыларын басқару бойынша функционалдылық Басқару серверінің ажырамас бөлігі болып табылады.
- Мәжбүрлеп табыстау (KCD) дұрыс жұмыс істеуі үшін Басқару сервері болып табылатын қабылдаушы тарап домендік есептік жазбада жұмыс істеуі керек.

http/kes4mob.mydom.local үшін Service Principal Name

KSCMobileSrvcUsr есептік жазбасы бар доменде, Басқару сервері бар құрылғының 13292-портында мобильді протокол сервисінің жариялануы үшін Service Principal Name (SPN) жазу керек. Басқару сервері бар kes4mob.mydom.local құрылғысы үшін бұл келесідей көрінетін болады:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Кері прокси-сервері бар құрылғылардың домен сипаттарын конфигурациялау (firewall.mydom.local)

Трафикті табыстау үшін кері прокси-сервері (firewall.mydom.local) бар құрылғыны SPN (http/kes4mob.mydom.local:13292) бойынша анықталған қызметке сеніп тапсыру қажет.

Кері прокси-сервері бар құрылғыны SPN (http/kes4mob.mydom.local:13292) бойынша анықталған қызметке сеніп тапсыру үшін, әкімші келесі әрекеттерді орындауы тиіс:

1. Microsoft Management Console "Active Directory Users and Computers" жабдықтарында кері прокси-сервері (firewall.mydom.local) орнатылған құрылғыны таңдаңыз.

2. **Delegation** қойыншасындағы құрылғының сипаттарында **Trust this computer for delegation to specified service only** қосқышы үшін **Use any authentication protocol** нұсқасын таңдау.

3. **Services to which this account can present delegated credentials** тізіміне SPN http/kes4mob.mydom.local:13292.

Жарияланым үшін ерекше (кастомизацияланған) сертификат (kes4mob.mydom.global)

Басқару серверінің мобильді протоколын жариялау үшін FQDN kes4mob.mydom.global мекенжайына арнайы (кастомизацияланған) сертификат шығару және оны әдепкі бойынша серверлік сертификаттың орнына Басқару консоліндегі Басқару сервері мобильді протоколының параметрлерінде көрсету керек. Бұл үшін, Басқару сервері сипаттары терезесінде, **Параметрлер** бөлімінде **Ұялы құрылғыларға арналған портты ашу** жалаушасын қою және ашылмалы тізімнен **Сертификат қосу** тармағын таңдау керек.

Серверлік сертификаты бар контейнерде (p12 немесе pfx кеңейтімі бар файл) түбірлік сертификаттар тізбегі (жария бөліктер) болуы керек екенін де ескеру қажет.

Кері прокси-серверге жариялауды баптау

Кері прокси-серверде ұялы құрылғы тарапынан kes4mob.mydom.global атты 13292-портқа баратын трафик үшін, FQDN kes4mob.mydom.global атауына арнап шығарылған серверлік сертификатты қолдану арқылы SPN http/kes4mob.mydom.local:13292 мекенжайына KCD конфигурациялау керек. Жарияланымда да, жарияланатын қатынасу нүктесінде де (Басқару серверінің 13292-порты) бірдей серверлік сертификат болуы керек екенін ескеру қажет.

Firebase Cloud Messaging қолдану

Kaspersky Security Center-де Android операциялық жүйесі басқаратын KES құрылғыларына пәрмендерді уақтылы жеткізу үшін push-нотификациялар механизмі пайдаланылады. KES құрылғылары мен Басқару сервері арасындағы push-нотификациялар Firebase Cloud Messaging (бұдан әрі – FCM) сервисінің көмегімен жүзеге асырылады. Kaspersky Security Center Басқару консолінде KES құрылғыларын осы сервиске қосу үшін Cloud Messaging сервисінің параметрлерін көрсете аласыз.

Firebase Cloud Messaging параметрлерін алу үшін Google есептік жазбаңыз болуы керек.

FCM қолдануды қосу үшін:

1. Басқару консолінен **Мобильді құрылғыларды басқару** түйіні мен **Ұялы құрылғылар** торабын таңдаңыз.

2. **Ұялы құрылғылар** қалтасының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.

3. Қалта сипаттары терезесінен **Firebase Cloud Messaging параметрлері** бөлімін таңдаңыз.

4. **Firebase жобасының нөмірі** өрісінде Sender ID FCM енгізіңіз.

5. **Жеке кілт файлы (JSON пішімінде)** өрісінде жеке кілт файлын таңдаңыз.

   Басқару серверімен келесі жолы синхрондау кезінде, Android операциялық жүйесі басқаратын KES құрылғылары Firebase Cloud Messaging қызметіне қосылатын болады.

Firebase Cloud Messaging параметрлерін **Параметрлер бастапқы мәнге келтірілуде** түймесі арқылы өзгерте аласыз.

Басқа Firebase жобасына ауысқанда, FCM жұмысы 10 минуттан кейін жалғасады.

FCM сервисі келесі мекенжайлар ауқымында жұмыс істейді:

- KES құрылғылары тарапынан 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), 5230 (HTTPS) порттарына келесі мекенжайлардан қатынасу мүмкіндігі қажет:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - немесе "Google ASN 15169" тізіміндегі барлық IP мекенжайларына
- Басқару сервері тарапынан 443-портқа (HTTPS) келесі мекенжайлардан қатынасу қажет:
  - fcm.googleapis.com
  - немесе "Google ASN 15169" тізіміндегі барлық IP мекенжайларына

Басқару консолінде Басқару серверінің сипаттарында прокси-сервердің параметрлері (**Қосымша** / **Интернет желісіне қатынасу параметрлері**) көрсетілген болса, олар FCM-мен өзара әрекеттесу үшін пайдаланылатын болады.

FCM орнату: Sender ID мен жабық кілт файлын алу

FCM конфигурациялау үшін:

1. Google порталында тіркелу.
2. Firebase консоліне өтіңіз.
3. Келесі әрекеттердің бірін орындаңыз:
   - Жобаны жасау үшін **Жоба жасау** түймесін басып, экрандағы нұсқауларды орындаңыз.
   - Бар жобаны ашыңыз.
4. Тегершік белгішесін басып, **Жоба параметрлері** тармағын таңдаңыз.

   Жоба параметрлері терезесі ашылады.
5. **Cloud Messaging** қойындысын таңдаңыз.

6. **Firebase Cloud Messaging API (V1)** бөліміндегі **Sender ID** өрісінен Sender ID көшіріп алыңыз.

7. **Қызметтің есептік жазбалары** қойындысын таңдап, **Жаңа жеке кілтті жасау** түймесін басыңыз.

8. Ашылған терезеде жеке кілт файлын жасау және жүктеп салу үшін **Кілтті жасау** түймесін басыңыз.

Firebase Cloud Messaging конфигурацияланған.

Жалпыға ортақ кілттер инфрақұрылымымен біріктіру

Жалпыға ортақ кілттер инфрақұрылымымен (Public Key Infrastructure, бұдан әрі PKI) біріктіру, ең алдымен Басқару серверінің домендік пайдаланушы сертификаттарын шығаруын жеңілдетуге арналған.

Әкімші Басқару консолінде пайдаланушыға домендік сертификат тағайындай алады. Мұны келесі тәсілдердің бірімен жасауға болады:

- пайдаланушыға сертификаттарды орнату шеберіндегі файлдан арнайы (кастомизацияланған) сертификат тағайындау;

- PKI-мен біріктіруді жүзеге асырыңыз және PKI инфрақұрылымын сертификаттардың белгілі бір түріне немесе сертификаттардың барлық түрлеріне арналған сертификат көзі етіп тағайындаңыз.

PKI-мен біріктіру параметрлері **Ашық кілттердің инфрақұрылымымен интеграциялау** сілтемесінен өткен кезде **Мобильді құрылғыларды басқару** / **Сертификаттар** қалтасының жұмыс аймағында қолжетімді.

Пайдаланушылардың домендік сертификаттарын шығару үшін PKI-мен біріктірудің жалпы қағидаты

Басқару консолінде, **Мобильді құрылғыларды басқару** / **Сертификаттар** қалтасының жұмыс аймағындағы **Ашық кілттердің инфрақұрылымымен интеграциялау** сілтемесі арқылы, домендік CA арқылы домендік пайдаланушы сертификаттарын шығару үшін Басқару сервері тарапынан қолданылатын домендік есептік жазбаны (бұдан әрі – PKI-мен біріктіру орындалатын есептік жазба) белгілеу керек.

Назар аударыңыз:

- PKI-мен біріктіру параметрлерінде сертификаттардың барлық түрлері үшін әдепкі бойынша үлгіні көрсету мүмкіндігі бар. Бұл арада, сертификаттарды шығару ережелерінде (ережелер **Мобильді құрылғыларды басқару** / **Сертификаттар** қалтасының жұмыс аймағында, **Сертификат беру ережелерін конфигурациялау** түймесі арқылы қолжетімді) әрбір сертификат түрі үшін бөлек үлгі жасау мүмкіндігі бар.

- Басқару сервері орнатылған құрылғыда PKI-мен біріктіру жүргізілетін есептік жазбаның сертификаттар қоймасында Enrollment Agent (EA) мамандандырылған сертификаты орнатылуы керек. Enrollment Agent (EA) сертификатын домендік CA (Certificate Authority) әкімшісі шығарады.

PKI-мен біріктіру жүргізілетін есептік жазба келесі критерийлерге сәйкес келуі керек:

- Домен пайдаланушысы болып табылады.

- Бұл PKI-мен біріктіру жүзеге асырылатын орнатылған Басқару сервері бар құрылғының жергілікті әкімшісі.

- *Қызмет ретінде жүйеге кіру* құқығы бар.
- Бұл есептік жазбаның астында тұрақты пайдаланушы профилін жасау үшін Басқару сервері орнатылған құрылғыны кем дегенде бір рет іске қосу қажет.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (бұдан әрі Веб-сервер) – Kaspersky Security Center құрамдасы. Веб-сервер жеке орнату пакеттерін, ұялы құрылғыларға арналған жеке орнату пакеттерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды жариялауға арналған.

Құрылған орнату пакеттері Веб-серверде автоматты түрде жарияланады және бірінші рет жүктегеннен кейін жойылады. Әкімші қалыптастырылған сілтемені пайдаланушыға кез келген ыңғайлы тәсілмен, мысалы, электрондық пошта арқылы жібере алады.

Алынған сілтеме арқылы, пайдаланушы ұялы құрылғыға арналған ақпаратты жүктей алады.

Веб-серверді конфигурациялау

Веб-Сервердің сипаттарында Веб-серверді дәл конфигурациялау үшін HTTP (8060) және HTTPS (8061) протоколдарының порттарын ауыстыруға болады. Сондай-ақ, порттарды ауыстырудан бөлек, HTTPS протоколы үшін серверлік сертификатты ауыстыруға және HTTP протоколы үшін веб-сервер FQDN атауын ауыстыруға болады.

Басқа да күнделікті тапсырмалар

Бұл бөлімде Kaspersky Security Center бағдарламасымен күнделікті жұмыс істеу бойынша ұсыныстар бар.

Басқару консолінде түс индикаторлары мен тіркелген оқиғаларды мониторингтеу

Басқару консолінде Kaspersky Security Center және басқарылатын құрылғылардың ағымдағы күйін түс индикаторлары арқылы жылдам бағалауға болады. Индикаторлар **Мониторинг** қойыншасындағы **Басқару сервері** торабының жұмыс аймағында көрсетіледі. Қойыншада түсті индикаторларға және тіркелген оқиғаларға ие алты ақпараттық блок бар. Түсті индикатор – панельдің сол жағындағы түсті тік жолақ. Индикаторы бар әрбір блок Kaspersky Security Center жеке функционалды аймағына жауап береді (төмендегі кестені қараңыз).

Басқару консолиндегі түсті индикаторлардың жауапкершілік аймақтары

Панель атауы	Түсті индикатордың жауапкершілік аймағы
Орналастыру	Ұйым желісіндегі құрылғыларға Желілік агент пен қауіпсіздік бағдарламаларын орнату.
Басқару схемасы	Басқару тобы құрылымы. Желіні сканерлеу. Құрылғыны жылжыту ережелері
Қорғаныс параметрлері	Қауіпсіздік бағдарламасының функциялары: қорғаныс күйі, зиянды БҚ іздеу.
Жаңарту	Жаңартулар және патчтар.

Панель атауы	Түсті индикатордың жауапкершілік аймағы
Мониторинг	Қорғаныс күйі
Басқару сервері	Басқару сервері функциялары мен сипаттары.

Индикаторда бес түстің бірі болуы мүмкін (төмендегі кестені қараңыз). Индикатордың түсі Kaspersky Security Center ағымдағы күйіне және тіркелген оқиғаларға байланысты.

Индикаторлардың түсті кодтамалары

Күй	Индикатор түсі	Индикатор түсінің мәні
Ақпараттық	Жасыл	Әкімшінің араласуы қажет емес.
Ескерту	Сары	Әкімшінің араласуы қажет.
Критикалық	Қызыл	Күрделі мәселелер бар. Оларды шешу үшін әкімшінің араласуы қажет.
Ақпараттық	Көгілдір	Басқарылатын құрылғылардың қауіпсіздігіне қауіп төндірмейтін оқиғалар тіркелді.
Ақпараттық	Сұр	Оқиға туралы ақпарат жоқ немесе әлі алынған жоқ.

Әкімші мақсаты – индикаторларды **Мониторинг** қойыншасының барлық ақпараттық тақталарында "жасыл" күйінде қолдау.

Ақпараттық тақталарда түс индикаторлары мен Kaspersky Security Center күйіне әсер ететін тіркелген оқиғалар да көрсетіледі (төмендегі кестені қараңыз).

Тіркелген оқиғалар индикаторының атауы, сипаттамасы және түсі

Индикатор түсі	Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Сипаттамасы
Қызыл	**%1 құрылғыда лицензияның жарамдылық мерзімі бітті**	IDS_AK_STATUS_LIC_EXPAIRED	Бұл түрдегі оқиғалар коммерциялық лицензияның мерзімі өткен кезде орын алады. Күніне бір рет Kaspersky Security Center бағдарламасы лицензияның лицензия мерзімінің өтпегенін тексеріп тұрады. Коммерциялық лицензияның мерзімі аяқталғаннан кейін, Kaspersky Security Center қолданбасы Базалық функционалдылық режимінде жұмыс істейді. Kaspersky Security Center бағдарламасын пайдалануды жалғастыру үшін коммерциялық лицензияның жарамдылық мерзімін ұзартыңыз.
Қызыл	**Қауіпсіздік бағдарламасы іске қосылмаған құрылғылардың саны: %1 құрылғы**	IDS_AK_STATUS_AV_NOT_RUNNING	Бұл түрдегі оқиғалар құрылғыда орнатылған қауіпсіздік бағдарламасы жұмыс істемей тұрғанда орын алады. Құрылғыда Kaspersky Endpoint Security бағдарламасы жұмыс істеп тұрғанын тексеріңіз.
Қызыл	**Қорғаныс өшірілген құрылғылардың саны: %1 құрылғы**	IDS_AK_STATUS_RTP_NOT_RUNNING	Бұл түрдегі оқиғалар құрылғыдағы қорғаныс бағдарламасы белгіленген уақыттан артық өшірілген кезде орын алады. Құрылғыдағы ағымдағы нақты уақыт режимінде қорғау күйін тексеріңіз және сізге қажет барлық қорғаныс құрамдастары қосылғанына көз жеткізіңіз.

Индикатор түсі	Оқиға түрінің көрсетілетін атауы	Оқиға түрі	Сипаттамасы
Қызыл	**Құрылғылардағы бағдарламалық жасақтамада осалдық анықталды**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Осы түрдегі оқиғалар *осалдықтарды және қажетті жаңартуларды іздеу* тапсырмасы құрылғыда орнатылған бағдарламаларда көрсетілген критикалық деңгейі бар осалдықтарды анықтаған кезде орын алады. Бағдарламаларды басқару қалтасының **Бағдарламалық жасақтама жаңартулары** ішкі қалтасында **қолжетімді жаңартулар тізімін тексеріңіз**. Бұл қалтада Microsoft корпорациясының және құрылғыларға таратылуы мүмкін басқа бағдарламалық жасақтама өндірушілерінің Басқару сервері алған жаңартулардың тізімі бар. Қолжетімді жаңартулар туралы ақпаратты қараңыз және оларды құрылғыңызға орнатыңыз.
Қызыл	**Критикалық оқиғалар Басқару серверінде тіркелді**	IDS_AK_STATUS_EVENTS_OCCURED	Бұл түрдегі оқиғалар Басқару серверінің критикалық оқиғалары анықталған кезде орын алады. Басқару серверінде сақталған оқиғалар тізімін тексеріңіз, содан кейін критикалық оқиғаларды рет-ретімен түзетіңіз.
Қызыл	**Басқару серверінің оқиғаларынан қателер тіркелді**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Бұл түрдегі оқиғалар Басқару сервері жағында күтпеген қателер тіркелгенде орын алады. Басқару серверінде сақталған оқиғалар тізімін тексеріңіз, содан кейін критикалық оқиғаларды рет-ретімен түзетіңіз.
Қызыл	**%1 құрылғыға қосылым жоғалды**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Бұл түрдегі оқиғалар Басқару сервері мен құрылғы арасындағы қосылым жоғалған кезде орын алады. Ажыратылған құрылғылар тізімін қарап шығыңыз және оларды қайта қосып көріңіз.
Қызыл	**%1 құрылғы Басқару серверіне ұзақ уақыт бойы қосылмаған**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Осы түрдегі оқиғалар құрылғы Басқару серверіне белгіленген уақыттан артық қосылмаған кезде орын алады, себебі құрылғы өшірулі. Құрылғының қосулы екенін және Желілік агент жұмыс істеп тұрғанын тексеріңіз.
Қызыл	**%1 құрылғының күйі «Бәрі дұрыс» күйінен басқаша**	IDS_AK_STATUS_HOST_NOT_OK	Бұл түрдегі оқиғалар Басқару серверіне қосылған *OK* құрылғысының күйі *Критикалық* немесе *Ескерту* күйіне өзгерген кезде орын алады. Ақаулықты Kaspersky Security Center қашықтан диагностикалау утилитасын пайдаланып шешуге болады.
Қызыл	**Дерекқорлар ескірген құрылғылардың саны: %1 құрылғы**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Бұл түрдегі оқиғалар құрылғыдағы антивирустық дерекқорлар белгілі бір уақыт аралығында жаңартылмаған кезде орын алады. Kaspersky антивирустық дерекқорларын жаңарту үшін нұсқауларды орындаңыз.
Қызыл	**Windows Update жаңартуларын тексеру орындалмағанына көп болған құрылғы(лар)дың саны: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Осы түрдегі оқиғалар *Windows Update синхрондау* тапсырмасы көрсетілген уақыттан артық орындалмаған кезде орын алады. Windows Update жаңартуларын Басқару серверімен синхрондау үшін нұсқауларды орындаңыз.
Қызыл	**Kaspersky Security Center арналған %1 плагин орнатылуы тиіс**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Бұл түрдегі оқиғалар Kaspersky бағдарламалары үшін қосымша плагиндерді орнату қажет болғанда орын алады. Kaspersky техникалық қолдау қызметінің веб-сайтынан Kaspersky бағдарламасы үшін қажетті басқару плагиндерін жүктеп алыңыз және орнатыңыз.

Басқарылатын құрылғыларға қашықтан қатынасу

Бұл бөлімде басқарылатын құрылғыларға қашықтан қатынасу туралы ақпарат бар.

Microsoft Windows on Arm жұмыс істейтін құрылғыдан Kaspersky Security Center Web Console веб-консоліне кірген кезде басқарылатын құрылғыларға қашықтан қосылу қолдау көрсетілмейді.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты байланысты қамтамасыз ету үшін "Басқару серверімен байланысты үзбеу" параметрін қолдану

Push-серверлерді қолданбасаңыз, онда Kaspersky Security Center бағдарламасы басқарылатын құрылғылар мен Басқару сервері арасында үздіксіз байланысты қамтамасыз етпейді. Басқарылатын құрылғылардағы Желілік агенттер мезгіл-мезгіл қосылым орнатып, Басқару серверімен синхрондалады. Мұндай синхрондау кезеңінің мерзімділігі Желілік агенттің саясатында белгіленеді. Ерте синхрондау қажет болса, онда Басқару сервері (немесе қажет болса, тарату нүктесі) қол қойылған желілік пакетті IPv4 желісі немесе IPv6 желісі арқылы Желілік агенттің UDP портына жібереді. Әдепкі бойынша порт нөмірі – 15000. Басқару серверінен басқарылатын құрылғыға UDP бойынша қосылу мүмкін болмаса, онда синхрондау әрекеті, синхрондау кезеңі ішінде Желілік агентті Серверге кезекті рет мезгіл-мезгіл қосу кезінде жүзеге асырылады.

Желілік агентті Басқару серверіне алдын ала қоспайынша, жергілікті тапсырмаларды іске қосу және тоқтату, басқарылатын бағдарлама бойынша статистиканы алу немесе туннель жасау сияқты кейбір операцияларды орындау мүмкін емес. Бұл мәселені шешу үшін, егер сіз push-серверлерді қолданбасаңыз, сіз басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылымды қамтамасыз ететін **Басқару серверімен байланысты үзбеу** параметрін қолдана аласыз.

Басқарылатын құрылғы мен Басқару сервері арасындағы тұрақты қосылымды қамтамасыз ету үшін:

1. Консоль ағашында **Басқарылатын құрылғылар** қалтасын таңдаңыз.
2. Қалтаның жұмыс аймағынан, тұрақты байланысты қамтамасыз еткіңіз келетін басқарылатын құрылғыны таңдаңыз.
3. Құрылғының мәнмәтіндік мәзірінен **Сипаттар** тармағын таңдаңыз.

   Таңдалған құрылғы сипаттары терезесі ашылады.
4. Ашылған терезенің **Жалпы** бөлімінде **Басқару серверімен байланысты үзбеу** параметрін таңдаңыз.

Басқарылатын құрылғы мен Басқару сервері арасында тұрақты қосылым орнатылған.

Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың жалпы саны 300-ден аспауы тиіс.

Құрылғыны Басқару серверіне қосу уақытын тексеру туралы

Құрылғы өшірілген кезде Желілік агент Басқару серверін өшіру туралы хабарлайды. Басқару консолінде мұндай құрылғы өшірулі болып көрсетіледі. Алайда, Агент барлық жағдайда Басқару серверіне хабарлай алмайды. Сол себепті, Басқару сервері әрбір құрылғы үшін ара-тұра **Басқару серверіне қосылған уақыты** атрибутын талдап тұрады (атрибуттың мәні Басқару консолінде, **Жалпы** бөліміндегі құрылғы сипаттарында көрсетіледі) және оны Желілік агенттің қолданыстағы параметрлерінен синхрондау кезеңімен салыстырады. Құрылғы үш синхрондау кезеңінен артық уақыт бойы байланысқа шықпаса, онда мұндай құрылғы өшірулі болып белгіленеді.

Мәжбүрлеп синхрондау туралы

Kaspersky Security Center бағдарламасы басқарылатын құрылғылар үшін күйді, параметрлерді, тапсырмаларды және саясаттарды автоматты түрде синхрондайтынына қарамастан, кейбір жағдайларда әкімші белгілі бір құрылғы үшін ағымдағы уақытта синхрондау орындалғанын нақты білуі керек.

Басқару консоліндегі басқарылатын құрылғылардың контекстік мәзірінде, мәзірдің **Барлық тапсырмалар** тармағында **Мәжбүрлеп синхрондау** пәрмені бар. Kaspersky Security Center 15.1 бағдарламасы осы пәрменді орындаған кезде, Басқару сервері құрылғыға қосылуға тырысады. Егер бұл әрекет сәтті болса, мәжбүрлеп синхрондау орындалады. Әйтпесе, мәжбүрлеп синхрондау Желілік агент Сервермен байланыс орнатқаннан кейін ғана орындалады.

Туннельдеу туралы

Kaspersky Security Center бағдарламасы Басқару консолінен TCP қосылымдарын Басқару сервері арқылы және одан әрі Желілік агент арқылы басқарылатын құрылғыдағы белгіленген портқа туннельдеуге мүмкіндік береді. Туннельдеу, егер Басқару консолі бар құрылғыны құрылғыға тікелей қосу мүмкін болмаса, Басқару консолі орнатылған құрылғыдағы клиент қолданбасын басқарылатын құрылғыдағы TCP портына қосу үшін қолданылады.

Атап айтқанда, туннельдеу қашықтағы жұмыс үстеліне қосылу үшін қолданылады: бұрыннан бар сессияға қосылу үшін де, жаңа қашықтағы сессияны құру үшін де.

Сондай-ақ, туннельдеуді сыртқы құралдар механизмі арқылы пайдалануға да болады. Атап айтқанда, әкімші осылайша putty утилитасын, VNC клиентін және басқа құралдарды іске қоса алады.

Өлшеу нұсқаулығы

Бұл нұсқаулықта Kaspersky Security Center бағдарламасын масштабтау туралы ақпарат ұсынылған.

Осы нұсқаулық туралы

Kaspersky Security Center 15.1 өлшеу нұсқаулығы (сондай-ақ, бұдан әрі Kaspersky Security Center), Kaspersky Security Center орнатуды және басқаруды жүзеге асыратын мамандарға және Kaspersky Security Center пайдаланатын ұйымдарға техникалық қолдау көрсететін мамандарға арналған.

Барлық ұсыныстар мен есептеулер, Kaspersky Security Center Kaspersky бағдарламалық жасақтамасы орнатылған құрылғылардың (соның ішінде ұялы құрылғылардың) қорғанысын басқаратын желілер үшін келтірілген. Ұялы (немесе кез келген басқа) басқарылатын құрылғылар болса, олар бөлек қарастырылуы керек, бұл мәселе арнайы келісіледі.

Әртүрлі жұмыс шарттарында оңтайлы өнімділікке қол жеткізу және оны сақтау үшін, желідегі құрылғылардың санын, желі топологиясын және өзіңізге қажетті Kaspersky Security Center функциялар жиынтығын ескеруіңіз қажет.

Нұсқаулықта келесі ақпарат келтірілген:

- Kaspersky Security Center шектеулері
- Kaspersky Security Center өзекті түйіндері – Басқару серверлері мен тарату нүктелері үшін есептеу туралы:
  - Басқару серверлері мен тарату нүктелеріне қойылатын аппараттық талаптар туралы
  - Басқару серверлерінің саны мен иерархиясын есептеу туралы
  - Тарату нүктелерінің саны мен конфигурациясын есептеу туралы
- Желідегі құрылғылар санына байланысты, дерекқордағы оқиғаларды сақтау параметрлерін конфигурациялау туралы
- Өнімділікті оңтайландыруға қатысты жалпы қабылданған озық тәжірибелер
- Kaspersky Security Center оңтайлы өнімділігін қамтамасыз ету үшін кейбір тапсырмалардың параметрлерін конфигурациялау туралы
- Kaspersky Security Center Басқару сервері мен әрбір қорғалатын құрылғы арасындағы трафикті (желіге түсетін жүктемені) тұтыну туралы

Бұл нұсқаулыққа келесі жағдайларда жүгіну ұсынылады:

- Kaspersky Security Center орнату алдында ресурстарды жоспарлау кезінде
- Kaspersky Security Center орналастырылған желі өлшемінің елеулі өзгерістерін жоспарлау кезінде

- Желінің шектеулі сегментінде (сынақ ортасы) Kaspersky Security Center-ді пайдаланудан корпоративтік желіде Kaspersky Security Center-ді толық ауқымды түрде орналастыруға көшкен кезде
- Kaspersky Security Center қолданылатын функциялары жиынтығына өзгерістер енгізілген кезде

Kaspersky Security Center шектеулері туралы ақпарат

Төмендегі кестеде Kaspersky Security Center ағымдағы нұсқасының шектеулері келтірілген.

Kaspersky Security Center шектеулері

Шектеу түрі	Мән
Бір Басқару серверіне шаққандағы басқарылатын құрылғылардың ең көп саны	100 000
Басқару серверімен байланысты үзбеу параметрі таңдалған құрылғылардың ең көп саны	300
Басқару топтарының ең көп саны	10 000
Сақталатын оқиғалардың ең көп саны	45 000 000
Саясаттардың ең көп саны	2000
Тапсырмалардың ең көп саны	2000
Active Directory нысандарының ең көп жиынтық саны (бөлімшелер мен пайдаланушылардың есептік жазбалары, құрылғылар және қауіпсіздік топтары)	1 000 000
Саясаттағы профильдердің ең көп саны	100
Бір негізгі Басқару серверіндегі қосалқы Серверлердің ең көп саны	500
Виртуалды Басқару серверлерінің ең көп саны	500
Бір тарату нүктесі қызмет көрсете алатын құрылғылардың ең көп саны (тарату нүктелері тек ұялы емес құрылғыларға қызмет көрсете алады)	10 000
Бір қосылымы шлюзін қолдана алатын құрылғылардың ең көп саны	10 000, ұялы құрылғылармен қоса
Бір Басқару серверіне шаққандағы ұялы құрылғылардың ең көп саны	100 000 минус тұрақты басқарылатын құрылғылар саны

Басқару серверлері үшін есептеулер

Бұл бөлімде Басқару серверлері ретінде пайдаланылатын құрылғыларға арналған аппараттық және бағдарламалық талаптар келтірілген. Сондай-ақ, ұйым желісінің конфигурациясына байланысты Басқару серверлерінің санын және олардың иерархиясын есептеу бойынша ұсыныстар берілген.

Басқару сервері үшін аппараттық ресурстарды есептеу

Бұл бөлімде Басқару серверіне арналған аппараттық ресурстарды жоспарлау кезінде басшылыққа алуға болатын есептеулер келтірілген. Осалдықтар мен патчтарды басқаруды пайдалану кезінде дискідегі орынды есептеу бойынша ұсыныс бөлек келтіріледі.

ДҚБЖ және Басқару серверіне арналған аппараттық талаптар

Төмендегі кестелерде тестілеу кезінде алынған ДҚБЖ мен Басқару серверінің ұсынылған минималды аппараттық талаптары келтірілген. Қолдау көрсетілетін операциялық жүйелер мен ДҚБЖ толық тізімі аппараттық және бағдарламалық талаптар тізбесінде келтірілген.

Басқару сервері мен ДҚБЖ әртүрлі құрылғыларда, желіде 50000 құрылғы бар

Басқару сервері бар құрылғының конфигурациясы

Жабдық	Мән
Процессор	4 ядро, 2500 МГц
ЖЖҚ	8 ГБ
Қатты диск	300 ГБ, RAID болғаны жөн
Желілік адаптер	1 Гбит

ДҚБЖ құрылғысының конфигурациясы

Жабдық	Мән
Процессор	4 ядро, 2500 МГц
ЖЖҚ	16 ГБ
Қатты диск	200 ГБ SATA RAID
Желілік адаптер	1 Гбит

Басқару сервері мен ДҚБЖ бір құрылғыда, желіде 50000 құрылғы бар

Басқару сервері және ДҚБЖ сервері бар құрылғы конфигурациясы

Жабдық	Мән
Процессор	8 ядро, 2500 МГц
ЖЖҚ	16 ГБ
Қатты диск	500 ГБ SATA RAID
Желілік адаптер	1 Гбит

Басқару сервері мен ДҚБЖ әртүрлі құрылғыларда, желіде 100000 құрылғы бар

Басқару сервері бар құрылғының конфигурациясы

Жабдық	Мән
Процессор	8 ядро, 2,13 ГГц
ЖЖҚ	8 ГБ
Қатты диск	1 ТБ, RAID
Желілік адаптер	1 Гбит

ДҚБЖ құрылғысының конфигурациясы

Жабдық	Мән
Процессор	8 ядро, 2,53 ГГц
ЖЖҚ	26 ГБ
Қатты диск	500 ГБ SATA RAID
Желілік адаптер	1 Гбит

Тестілеу келесі конфигурациялармен жүргізілді:

- Басқару серверінде тарату нүктелерін автоматты түрде тағайындау қосылған немесе тарату нүктелері ұсынылған кестеге сәйкес қолмен тағайындалған;
- сақтық көшірме жасау тапсырмасы сақтық көшірмелерді бөлек серверде орналасқан файлдық ресурсқа сақтайды;
- Желілік агенттердің синхрондау кезеңі төмендегі кестеге сәйкес конфигурацияланған.

Желілік агенттерді синхрондау кезеңі

Синхрондау кезеңі, минуттар	Басқарылатын құрылғылардың саны
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Дерекқорда орынды есептеу

Дерекқордағы орынды келесі формула бойынша шамамен бағалауға болады:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), КБ,

мұндағы

- "C" – құрылғылар саны.

  Егер басқарылатын құрылғылар құрамында динамикалық виртуалды машиналар болса, онда "C" — бұл динамикалық емес басқарылатын құрылғылар саны мен **Басқару серверіне техникалық қызмет көрсету** тапсырмасының екі рет қатар іске қосылуы аралығында жасалған, Желілік агенті бар динамикалық виртуалды машиналар санының қосындысы.

- "E" – сақталатын оқиғалар саны.
- "A" – Active Directory нысандарының жиынтық саны:
  - Құрылғылардың есептік жазбалары
  - Пайдаланушы есептік жазбалары

- Қауіпсіздік топтарының есептік жазбалары
- Active Directory бөлімшелері

Active Directory сканерлеу өшірулі болса, онда "A" нөлге тең болып саналуы керек.

- N – соңғы құрылғыдағы түгенделетін орындалатын файлдардың орташа саны.
- F – орындалатын файлдар түгенделген соңғы құрылғылардың саны.

Егер сіз Kaspersky Endpoint Security саясатының параметрлерінде Басқару серверін іске қосылатын бағдарламалар туралы хабардар етуді қосуды жоспарласаңыз, онда іске қосылатын бағдарламалар туралы ақпаратты дерекқорда сақтау үшін қосымша (0,03 * C) ГБ қажет болады.

Басқару сервері Windows жаңартуларын таратса (Windows Server Update Services рөлін атқарады), онда дерекқорда қосымша 2,5 ГБ қажет болады.

Жұмыс барысында, дерекқорда *бос кеңістік* (unallocated space) деп аталатын орын пайда болады. Сондықтан, дерекқор файлының нақты өлшемі ("SQL Server" ДҚБЖ қолданған жағдайда, әдепкі бойынша KAV.MDF файлы) көбінесе дерекқордағы бос емес орыннан шамамен екі есе көп болады.

Транзакциялар журналының өлшемін нақты шектеу ұсынылмайды (егер сіз SQL Server серверін ДҚБЖ ретінде қолдансаңыз, әдепкі бойынша KAV_log.LDF файлы). MAXSIZE параметрінің әдепкі мәнін қалдыру ұсынылады. Алайда осы файлдың өлшеміне қатысты шектеу болса, KAV_log.LDF үшін MAXSIZE параметрінің әдеттегі қажетті минималды мәні 20480 МБ екенін ескеріңіз.

Дискідегі орынды есептеу (Осалдықтар мен патчтарды басқаруды пайдалануды ескере отырып және есепке алмай)

Осалдықтар мен патчтарды басқаруды пайдалануды есепке алмай, дискідегі орынды есептеу

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit қалтасы үшін қажетті Басқару серверіндегі орын шамамен келесі формула бойынша есептелуі мүмкін:

(724 * C + 0.15 * E + 0.17 * A), КБ

мұндағы

- "C" – құрылғылар саны.

  Егер басқарылатын құрылғылар құрамында динамикалық виртуалды машиналар болса, онда "C" — бұл динамикалық емес басқарылатын құрылғылар саны мен **Басқару серверіне техникалық қызмет көрсету** тапсырмасының екі рет қатар іске қосылуы аралығында жасалған, Желілік агенті бар динамикалық виртуалды машиналар санының қосындысы.

- "E" – сақталатын оқиғалар саны.

- "A" – Active Directory нысандарының жиынтық саны:
  - Құрылғылардың есептік жазбалары
  - Пайдаланушы есептік жазбалары
  - Қауіпсіздік топтарының есептік жазбалары
  - Active Directory бөлімшелері

Active Directory сканерлеу өшірулі болса, онда "A" нөлге тең болып саналуы керек.

Осалдықтар мен патчтарды басқаруды пайдалануды ескере тырып, дискідегі қосымша орынды есептеу

- Жаңартулар. Ортақ қатынасы бар қалтада жаңартуларды сақтау үшін қосымша кемінде 4 ГБ қажет.
- Орнату пакеттері. Басқару серверінде ортақ қатынасы бар қалтада орнату пакеттері болған кезде орнатылатын қолда бар орнату пакеттерінің жиынтық өлшеміне тең келетін қосымша орын қажет болады.
- Қашықтан орнату тапсырмалары. Басқару серверінде қашықтан орнату тапсырмалары болған кезде, дискіде орнатылатын орнату пакеттерінің жиынтық өлшеміне тең келетін қосымша орын керек болады (%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit қалтасында).
- Патчтар. Басқару сервері патчтарды орнату үшін қолданылса, онда дискіде қосымша орын керек болады:
  - Патчтарды сақтауға арналған қалтада барлық жүктелген патчтардың жиынтық өлшеміне тең келетін диск кеңістігі көлемі болуы керек. Әдепкі бойынша, патчтар %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles қалтасында сақталады.

    Патчтарды сақтауға арналған басқа қалтаны көрсету үшін klsrvswch утилитасын пайдалануға болады. klsrvswch утилитасы Басқару серверінің орнату қалтасында орналасқан. Әдепкі бойынша орнату жолы: <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    Басқару сервері WSUS ретінде қолданылса, онда осы қалта үшін кемінде 100 ГБ резервтеу ұсынылады.
  - %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit қалтасында – жаңартуларды (патчтарды) орнату және осалдықты түзету тапсырмасының қолда бар даналары сілтеме жасайтын патчтардың жиынтық өлшеміне тең келетін орын саны.

Басқару серверлерінің саны мен конфигурациясын есептеу

Негізгі Басқару серверіндегі жүктемені азайту үшін, әр басқару тобына жеке Басқару серверін тағайындауға болады. Негізгі Серверге бағынатын Басқару серверлерінің саны 500-ден аспауы керек.

Басқару серверлерінің конфигурациясын ұйымыңыздағы желінің қалай конфигурацияланғанына байланысты құру ұсынылады.

Динамикалық виртуалды машиналарды Kaspersky Security Center бағдарламасына қосу бойынша ұсыныстар

Динамикалық виртуалды машиналар статикалық виртуалды машиналарға қарағанда көбірек ресурстарды пайдаланады.

Динамикалық виртуалды машиналар туралы қосымша ақпаратты Динамикалық виртуалды машиналарды қолдау бөлімінен қараңыз.

Жаңа динамикалық виртуалды машинаны қосқанда, Kaspersky Security Center бағдарламасы Басқару консолінде осы динамикалық виртуалды машинаның белгішесін жасайды және динамикалық виртуалды машинаны басқару тобына жылжытады. Содан соң, динамикалық виртуалды машина Басқару сервері дерекқорына қосылады. Басқару сервері осы динамикалық виртуалды машинада орнатылған Желілік агентпен толық синхрондалған.

Ұйымның желісінде Желілік агент әрбір динамикалық виртуалды машина үшін келесі желілік тізімдерді жасайды:

- Жабдық
- Орнатылған бағдарламалық жасақтама
- Анықталған осалдықтар
- Бағдарламаларды басқару құрамдасының оқиғалары мен орындалатын файл тізімдері

Желілік агент осы желілік тізімдерді Басқару серверіне жібереді. Желілік тізімдердің өлшемі динамикалық виртуалды машинада орнатылған құрамдастарға байланысты, сондай-ақ Kaspersky Security Center және дерекқорларды басқару жүйесінің (ДҚБЖ) өнімділігіне әсер етуі мүмкін. Жүктеме сызықты емес түрде өсуі мүмкін екенін ескеріңіз.

Пайдаланушы динамикалық виртуалды машинамен жұмыс істеп, оны өшіргеннен кейін, бұл машина виртуалды инфрақұрылымнан жойылады, ол туралы жазбалар Басқару сервері дерекқорынан жойылады.

Бұл әрекеттердің барлығы Kaspersky Security Center бағдарламасы мен Басқару сервері дерекқорының көп ресурсын пайдаланады әрі Kaspersky Security Center және ДҚБЖ өнімділігін төмендетуі мүмкін. Kaspersky Security Center бағдарламасына 20 000-ға дейін динамикалық виртуалды машинаны қосу ұсынылады.

Қосылған динамикалық виртуалды машиналар стандартты операцияларды орындаса (мысалы, дерекқорды жаңарту) және ең көбі жадтың 80%-н және қолжетімді ядролардың 75-80%-н тұтынса, Kaspersky Security Center бағдарламасына 20 000-нан астам динамикалық виртуалды машинаны қосуға болады.

Динамикалық виртуалды машинада саясат, бағдарламалық жасақтама немесе операциялық жүйе параметрлерін өзгерту ресурстарды тұтынуды азайтуы немесе арттыруы мүмкін. Ресурстардың 80-95%-н тұтыну оңтайлы болып саналады.

Тарату нүктелері мен қосылым шлюздеріне арналған есептеулер

Бұл бөлімде тарату нүктелері ретінде пайдаланылатын құрылғыларға қойылатын аппараттық талаптар және ұйым желісінің конфигурациясына байланысты тарату нүктелері мен қосылым шлюздерінің санын есептеу бойынша ұсыныстар берілген.

Тарату нүктесі үшін талаптар

10 000-ға дейінгі клиент құрылғысын өңдеу үшін, тарату нүктесі келесі минималды талаптарға сай болуы керек (сынақ стендінің конфигурациясы ұсынылған):

- Процессор: Intel Core™ i7-7700 CPU, 3,60 ГГц, 4 ядро.
- Жедел жад: 8 ГБ.
- Дискідегі бос орын: 120 ГБ.

> Басқару серверін тарату нүктесі ретінде тағайындамаған жөн, себебі басқару серверіне түсетін жүктеме артады.

Басқару серверінде қашықтан орнату тапсырмалары болған жағдайда, тарату нүктесі бар құрылғыда орнатылатын орнату пакеттерінің жиынтық өлшеміне тең келетін диск кеңістігі қосымша түрде қажет болады.

Басқару серверінде жаңартуларды (патчтарды) орнату және тарату нүктесі бар құрылғыдағы осалдықтарды түзету тапсырмасының бір немесе бірнеше данасы болған кезде барлық орнатылатын патчтардың екі еселенген жиынтық өлшеміне тең диск кеңістігі қосымша түрде қажет болады.

Егер тарату нүктелері дерекқорлар мен бағдарлама модульдеріне жаңартуларды тікелей Kaspersky жаңарту серверлерінен алатын схеманы пайдалансаңыз, тарату нүктелері интернет желісіне қосылған болуы керек.

Тарату нүктелерінің саны мен конфигурациясын есептеу

Желіде клиент құрылғылары неғұрлым көп болса, тарату нүктелері да соғұрлым көп қажет болады. Тарату нүктелерін автоматты түрде тағайындауды өшірмеу ұсынылады. Тарату нүктелерін автоматты түрде тағайындау қосылған кезде, егер клиент құрылғыларының саны айтарлықтай көп болса, Басқару сервері тарату нүктелерін тағайындайды және олардың конфигурациясын анықтайды.

Арнайы бөлінген тарату нүктелерін пайдалану

Егер сіз тарату нүктелері ретінде белгілі бір құрылғыларды (мысалы, бұл үшін бөлінген серверлер) пайдалануды жоспарласаңыз, онда тарату нүктелерін автоматты түрде тағайындауды пайдаланбауға болады. Бұл жағдайда, тарату нүктелері ретінде тағайындағыңыз келетін құрылғыларда дискіде жеткілікті бос орын бар екеніне, олар үнемі өшірілмейтініне және "ұйқы режимі" өшірілгеніне көз жеткізіңіз.

Желілік құрылғылардың санына байланысты бір сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Желілік құрылғылардың санына байланысты бірнеше сегменті бар желідегі бірегей тағайындалған тарату нүктелерінің саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–100	1
100-нан артық	Қолайлы: (N/10 000 + 1), ұсынылады: (N/5000 + 2), мұндағы N желідегі құрылғылар саны

Клиент құрылғыларын (жұмыс станцияларын) тарату нүктелері ретінде пайдалану

Егер сіз әдеттегі клиент құрылғысын (жұмыс станциясын) тарату нүктесі ретінде пайдалануды жоспарласаңыз, байланыс арналары мен Басқару серверіне шамадан тыс жүктемені болдырмау үшін төмендегі кестеде көрсетілгендей тарату нүктесін тағайындау ұсынылады:

Желілік құрылғылардың санына байланысты желінің бір сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегменттерінің әрқайсысындағы клиент құрылғыларының саны	Тарату нүктелерінің саны
300-нан кем	0 (тарату нүктелері керек емес)
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Желілік құрылғылардың санына байланысты желінің бірнеше сегментін қамтитын желідегі тарату нүктелерінің рөлін атқаратын жұмыс станцияларының саны

Желі сегментіндегі клиент құрылғыларының саны	Тарату нүктелерінің саны
10-нан кем	0 (тарату нүктелері керек емес)
10–30	1
31–300	2
300-нан артық	(N/300 +1), мұндағы N – желідегі құрылғылардың саны; кемінде 3 тарату нүктесі

Егер тарату нүктесі өшірілген болса немесе басқа себептерге байланысты қолжетімді болмаса, онда басқарылатын құрылғылар жаңартулар алу үшін осы тарату нүктесінің әрекет ету ауқымынан Басқару серверіне жүгіне алады.

Қосылым шлюздерінің санын есептеу

Егер сіз қосылым шлюзін пайдалануды жоспарласаңыз, бұл функция үшін бөліп берілген құрылғыны пайдалану ұсынылады.

Бір қосылым шлюзі ұялы құрылғыларды қосқанда 10 000-нан аспайтын басқарылатын құрылғыларға қызмет етеді.

Тапсырмалар мен саясаттар үшін оқиғалар туралы ақпаратты сақтау

Бұл бөлімде Басқару сервері дерекқорында оқиғаларды сақтаумен байланысты есептеулер келтірілген және оқиғалар санын азайту және осылайша Басқару серверіне түсетін жүктемені азайту бойынша ұсыныстар берілген.

Әдепкі бойынша, әр тапсырманың және әр саясаттың сипаттарында тапсырманы орындауға және саясатты қолдануға байланысты барлық оқиғалардың журналында сақталуы көрсетілген.

Алайда, егер тапсырма жеткілікті жиі (мысалы, аптасына бір реттен көп) және құрылғылардың жеткілікті көп санында (мысалы, 10 000-нан астам) іске қосылса, оқиғалар саны тым көп болуы және оқиғалар дерекқорды толтыруы мүмкін. Бұл жағдайда, тапсырманың сипаттарында қалған екі нұсқаның бірін көрсету ұсынылады:

- **Тапсырманы орындау барысына қатысты оқиғаларды сақтау**. Бұл жағдайда, тапсырма орындалған әрбір құрылғыдан дерекқорға тек тапсырманың іске қосылуы, оның барысы және оның орындалуы туралы ақпарат келеді (сәтті, ескертумен немесе қатемен).

- **Тек тапсырманы орындау нәтижелерін сақтау**. Бұл жағдайда, тапсырма орындалған әрбір құрылғыдан дерекқорға тек тапсырманың орындалуы туралы ақпарат (сәтті, ескертумен немесе қатемен) келеді.

Егер саясат құрылғылардың жеткілікті көп саны үшін анықталса (мысалы, 10 000-нан астам), оқиғалар саны да тым көп болуы және оқиғалар дерекқорды толтыруы мүмкін. Бұл жағдайда, саясат сипаттарында тек маңызды оқиғаларды таңдап, оларды сақтауды қосу ұсынылады. Барлық басқа оқиғаларды сақтауды өшіру ұсынылады.

Осылайша, сіз дерекқордағы оқиғалардың санын азайтасыз, дерекқордағы оқиғалар кестесін талдаумен байланысты сценарийлердің жұмыс жылдамдығын арттырасыз және критикалық оқиғаларды оқиғалардың көп санымен ығыстыру қаупін азайтасыз.

Сондай-ақ, тапсырмаға немесе саясатқа қатысты оқиғаларды сақтау мерзімін қысқартуға болады. Әдепкі бойынша, бұл мерзім тапсырмамен байланысты оқиғалар үшін жеті күнді және саясатқа қатысты оқиғалар үшін 30 күнді құрайды. Сақтау мерзімі өзгерген кезде ұйымыңызда қабылданған жұмыс тәртібін және жүйе әкімшісінің әрбір оқиғаны талдауға қанша уақыт бөле алатынын ескеріңіз.

Оқиғаларды сақтау параметрлеріне келесі жағдайлардың кез келгенінде өзгерістер енгізген жөн:

- топтық тапсырмалардың аралық күйлерінің өзгеруі туралы және саясаттарды қолдану туралы оқиғалар Kaspersky Security Center дерекқорындағы барлық оқиғалардың едәуір пайызын алады;

- Kaspersky Event журналында, дерекқорда сақталатын оқиғалардың жалпы санына белгіленген шектен асқан кезде оқиғаларды автоматты түрде жою туралы жазбалар пайда болады.

Күніне бір құрылғыдан келетін оқиғалардың оңтайлы саны 20-дан аспауы керек деген негізде оқиғаларды тіркеу параметрлерін таңдаңыз. Қажет болса, желіңіздегі құрылғылар саны салыстырмалы түрде аз болған жағдайда ғана (10 000-нан аз), оқиғалардың ең көп санын аздап көбейтуге болады.

Кейбір тапсырмалардың ерекшеліктері мен оңтайлы параметрлері

Кейбір тапсырмалар желідегі құрылғылар санымен байланысты ерекшеліктерге ие. Бұл бөлімде осындай тапсырмалар үшін параметрлерді оңтайлы конфигурациялау бойынша ұсыныстар берілген.

Құрылғыларды анықтау, деректерді сақтық көшірмелеу тапсырмасы, Басқару серверіне қызмет көрсету тапсырмасы және Kaspersky Endpoint Security жаңарту топтық тапсырмалары Kaspersky Security Center базалық функционалдығына кіреді.

Құрылғыны табу жиілігі

Әдепкі бойынша белгіленген құрылғыларды іздеу жиілігін арттыру ұсынылмайды, себебі бұл доменнің контроллерлеріне шамадан тыс жүктеме түсіруі мүмкін. Керісінше, сіздің ұйымыңыздың қажеттіліктері мүмкіндік беретін ең төменгі жиілікпен сауалнама өткізу кестесін белгілеу ұсынылады. Төмендегі кестеде оңтайлы кестені есептеу бойынша ұсыныстар берілген.

Құрылғыларды анықтау кестесі

Желідегі құрылғылардың саны	Құрылғыларды табу үшін ұсынылатын жиілік
10,000-нан кем	Әдепкі бойынша белгіленген немесе сирек
10 000 және одан да көп	Тәулігіне бір рет немесе сирек

Басқару сервері деректерінің резервтік қоймасы және Басқару серверіне қызмет көрсету тапсырмалары

Басқару сервері келесі тапсырмаларды орындау кезінде жұмысын тоқтатады:

- Басқару сервері деректерінің сақтық көшірмесін жасау
- Басқару серверіне техникалық қызмет көрсету

Бұл тапсырмалар орындалып жатқанда, деректер дерекқорға келіп түсе алмайды.

Осы тапсырмалардың кестесін, олардың орындалуы уақыт бойынша Басқару серверінің басқа тапсырмаларын орындаумен қиылыспайтындай етіп өзгерту керек болуы мүмкін.

Kaspersky Endpoint Security жаңарту топтық тапсырмалары

Жаңартулар көзі Басқару сервері болса, онда Kaspersky Endpoint Security 10 және одан да жоғары нұсқасын жаңартудың топтық тапсырмалары үшін, **Тапсырманы іске қосуды тарату үшін аралықты автоматты түрде анықтау** жалаушасы қойылған **Қоймаға жаңартуларды жүктеу кезінде** кестесі ұсынылады.

Kaspersky серверлерінен жаңартуларды қоймаға жүктеу жергілікті тапсырмасын әрбір тарату нүктесінде жасаған болсаңыз, онда Kaspersky Endpoint Security жаңартудың топтық тапсырмасы үшін мерзімді кестені белгілеу ұсынылады. Бұл жағдайда, автономизация кезеңінің мәні бір сағатты құрауы тиіс.

Түгендеу тапсырмасы

Орнатылған файлдар туралы ақпаратты алу арқылы дерекқорға түсетін жүктемені азайтуға болады. Ол үшін, Kaspersky Endpoint Security бағдарламасына арналған түгендеу тапсырмасын стандартты бағдарламалар жинағы орнатылған бірнеше эталондық құрылғыларда орындау ұсынылады.

Басқару сервері бір құрылғыдан алынатын орындалатын файлдар саны 150 000-нан аса алмайды. Осы шектеуге жеткеннен кейін, Kaspersky Security Center жаңа файлдарды алмайды.

Әдеттегі клиент құрылғысындағы файлдар саны, әдетте, 60 000-нан аспайды. Файл серверіндегі орындалатын файлдардың саны үлкенірек болуы және тіпті 150 000 шегінен асып кетуі мүмкін.

Сынақ өлшемдері Kaspersky Endpoint Security 11 бағдарламасы орнатылған және ешқандай үшінші тарап бағдарламалары орнатылмаған Windows 7 операциялық жүйесі басқаратын құрылғыда түгендеу тапсырмасының нәтижелері келесідей екенін көрсетті:

- **DLL модульдерін түгендеу** және **Скрипт файлдарын түгендеу** жалаушалары алынып тасталса: шамамен 3000 файл.
- **DLL модульдерін түгендеу** және **Скрипт файлдарын түгендеу** жалаушалары қойылса: орнатылған операциялық жүйені жаңарту пакеттерінің санына байланысты 10 000-нан 20 000-ға дейінгі файл.
- **Скрипт файлдарын түгендеу** жалаушасы ғана қойылса: шамамен 10 000 файл.

Басқару сервері мен қорғалатын құрылғылар арасында желіге түсетін жүктеме туралы ақпарат

Бұл бөлімде өлшеулер жүргізілген шарттарды көрсете отырып, желідегі трафикті сынап өлшеу нәтижелері келтіріледі. Сіз осы ақпаратты ұйымның ішіндегі (немесе қорғалатын құрылғылары орналасқан ұйым мен Басқару сервері арасында) арналардың желілік инфрақұрылымы мен өткізу қабілетін жоспарлау кезінде анықтамалық ақпарат ретінде пайдалана аласыз. Сондай-ақ, желінің өткізу қабілетін біле отырып, сіз деректерді берумен байланысты белгілі бір операцияны орындауға қанша уақыт кететінін долбарлап бағалай аласыз.

Әртүрлі сценарийлерді орындау кезіндегі трафик шығыны

Төмендегі кестеде әртүрлі сценарийлерді орындау кезінде Басқару сервері мен басқарылатын құрылғы арасындағы трафикті сынап өлшеу нәтижелері келтірілген.

Құрылғыны Басқару серверімен синхрондау әдепкі бойынша 15 минут сайын немесе одан сирек болады. Алайда, егер сіз Басқару серверінде саясат немесе тапсырма параметрлерін өзгертсеңіз, онда осы саясат (немесе тапсырма) қолданылатын құрылғыларды мерзімінен бұрын синхрондау жүзеге асырылады және жаңа параметрлер құрылғыларға беріледі.

Басқару сервері мен басқарылатын құрылғы арасындағы трафик

Сценарий	Серверден әрбір басқарылатын құрылғыға дейінгі трафик	Әрбір басқарылатын құрылғыдан Серверге дейінгі трафик
Дерекқорлары жаңартылған Kaspersky Endpoint Security 11.7 for Windows бағдарламасын орнату	390 МБ	3.3 МБ
Желілік агентті орнату	75 МБ	397 КБ
Желілік агент пен Kaspersky Endpoint Security 11.7 for Windows бағдарламасын бірлесіп орнату	459 МБ	3.6 МБ
Пакеттегі дерекқорларды жаңартпай, антивирустық дерекқорларды бастапқы жаңарту (Kaspersky Security Network-ке қатысу өшірілсе)	113 МБ	1,8 МБ
Антивирустық дерекқорларды тәулік сайын жаңарту (Kaspersky Security Network-ке қатысу өшірілсе)	22 МБ	373 МБ
Құрылғыдағы дерекқорларды жаңартқанға дейін бастапқы синхрондау (саясат пен тапсырмаларды беру)	382 КБ	446 КБ
Құрылғыдағы дерекқорларды жаңартқаннан кейін бастапқы синхрондау	20 КБ	157 КБ
Басқару серверінде өзгертулер болмаған кезде синхрондау (кесте бойынша)	18 КБ	23 КБ
Топ саясатында бір параметр өзгерген кезде синхрондау (мерзімінен бұрын, өзгерту енгізілгеннен кейін бірден)	19 КБ	20 КБ
Топтық тапсырмада бір параметр өзгертілгеннен кейін синхрондау (мерзімінен бұрын, өзгерту енгізілгеннен кейін бірден)	14 КБ	11 КБ
Мәжбүрлеп синхрондау	110 КБ	109 КБ
Вирус анықталды оқиғасы (1 вирус)	44 КБ	50 КБ
Вирус анықталды оқиғасы (10 вирус)	58 КБ	77 КБ
Бағдарламалар тізімдемесі кестесін қосқаннан кейінгі бір реттік трафик	10 КБ-қа дейін	12 КБ-қа дейін
Бағдарламалар тізімдемесі тізімі қосылған кездегі күн сайынғы трафик	840 КБ-қа дейін	1 МБ-қа дейін

Трафиктің тәулік ішіндегі орташа шығыны

Басқару сервері мен басқарылатын құрылғы арасындағы тәулігіне орташа трафик шығыны:

- Серверден басқарылатын құрылғыға дейінгі трафик – 840 КБ.
- Басқарылатын құрылғыдан Серверге дейінгі трафик – 1 МБ.

Трафик келесі жағдайларда өлшенді:

- Басқарылатын құрылғыға Желілік агент және Kaspersky Endpoint Security 11.6 for Windows орнатылды.
- Құрылғы тарату нүктесі болып тағайындалмаған.
- Осалдықтар мен патчтарды басқару қосылмаған.
- Басқару серверімен синхрондау кезеңі 15 минутты құрады.

Техникалық қолдау қызметіне жүгіну

Бұл бөлімде техникалық қолдауды алу тәсілдері мен шарттары туралы ақпарат бар.

Техникалық қолдау алу жолдары

Егер сіз Kaspersky Security Center құжаттамасында немесе бағдарлама туралы басқа ақпарат көздерінде өз сұрағыңыздың шешімін таппаған болсаңыз, Kaspersky Техникалық қолдау қызметіне хабарласыңыз. Техникалық қолдау қызметінің қызметкерлері Kaspersky Security Center орнату және пайдалану туралы сұрақтарыңызға жауап береді.

> Kaspersky ұйымы Kaspersky Security Center бағдарламасы оның өмірлік циклі бойы қолдау көрсетеді (бағдарламалардың өмірлік циклі бетін қараңыз). Техникалық қолдау қызметіне хабарласпас бұрын техникалық қолдау көрсету ережелерімен танысыңыз.

Сіз Техникалық қолдау қызметінің мамандарымен келесі тәсілдердің бірімен байланыса аласыз:

- Техникалық қолдау қызметінің веб-сайтына кіру
- Kaspersky CompanyAccount порталынан техникалық қолдау қызметіне сұрау жіберу арқылы

Kaspersky CompanyAccount арқылы техникалық қолдау

Kaspersky CompanyAccount – бұл Kaspersky бағдарламаларын қолданатын ұйымдарға арналған портал. Kaspersky CompanyAccount порталы пайдаланушылардың Kaspersky мамандарымен электрондық сұрау салу арқылы өзара іс-қимыл жасауына арналған. Kaspersky CompanyAccount порталында электрондық сұрауларды Kaspersky мамандары тарапынан өңдеу күйін қадағалап, электрондық сұраулардың тарихын сақтауға болады.

Сіз өзіңіздің ұйымыңыздың барлық қызметкерлерін бір Kaspersky CompanyAccount есептік жазбасының шеңберінде тіркей аласыз. Бір есептік жазба, сізге тіркелген қызметкерлерден Kaspersky ұйымына жіберілген электронды сұрауларды орталықтан басқаруға, сондай-ақ Kaspersky CompanyAccount порталында осы қызметкерлердің құқықтарын басқаруға мүмкіндік береді.

Kaspersky CompanyAccount порталы келесі тілдерде қолжетімді:

- Ағылшын тілі
- Испан тілі
- Итальян тілі
- Неміс тілі
- Поляк тілі
- Португал тілі

- Орыс тілі
- Француз тілі
- Жапон тілі

Kaspersky CompanyAccount туралы толығырақ Техникалық қолдау қызметі веб-сайтынан біле аласыз.

Басқару серверінің қоқыс файлдарын алу

Басқару серверінің қоқыс файлдары белгілі бір уақытта Басқару сервері процестері туралы барлық ақпаратты қамтиды. Басқару серверінің қоқыс файлдары %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps қалтасында сақталады. Қоқыс файлдары Kaspersky Security Center пайдаланылған кезде сақталады және қолданба жойылған кезде біржола жойылады. Қоқыс файлдары Kaspersky автоматты түрде жіберілмейді.

Басқару серверінде ақаулық болса, Kaspersky техникалық қолдау қызметіне хабарласуға болады. Техникалық қолдау қызметінің маманы Kaspersky әрі қарай талдау үшін Басқару серверінің қоқыс файлдарын жіберуді сұрауы мүмкін.

Қоқыс файлдарында жеке деректер болуы мүмкін. Оны Kaspersky жібермес бұрын ақпаратты рұқсатсыз кіруден қорғау ұсынылады.

Бағдарлама мәліметтері көздері

Kaspersky веб-сайтындағы Kaspersky Security Center беті

Kaspersky Security Center бетінде бағдарлама, оның мүмкіндіктері мен жұмыс ерекшеліктері туралы мәлімет ала аласыз.

Білім базасындағы Kaspersky Security Center беті

Білім базасы – Kaspersky Техникалық қолдау қызметі веб-сайтындағы бөлім.

Білім базасындағы Kaspersky Security Center бетінде бағдарламаны сатып алу, орнату және қолдану туралы пайдалы ақпаратты, ұсыныстарды және жиі қойылатын сұрақтарға жауаптарды қамтитын мақалаларды таба аласыз.

Білім базасындағы мақалалар Kaspersky Security Center және Kaspersky басқа да бағдарламаларымен байланысты сұрақтарға жауап бере алады. Сонымен қатар, Білім базасының мақалаларында Техникалық қолдау қызметі жаңалықтары болуы мүмкін.

Kaspersky бағдарламаларын пайдаланушылар қауымдастығында талқылау

Сіздің сұрағыңызға тез арада жауап беру қажет болмаса, сіз оны Kaspersky мамандарымен және біздің форумдағы басқа да пайдаланушылармен талқылай аласыз.

Пайдаланушылар форумында, сіз жарияланған тақырыптарды қарай аласыз, өз пікірлеріңізді қалдыра аласыз, талқылау үшін жаңа тақырыптарды жасай аласыз.

> Онлайн-анықтаманы көрсету үшін интернет қосылымы керек.

Мәселеңіздің шешімін таба алмасаңыз, Техникалық қолдау қызметіне хабарласыңыз.

Глоссарий

Amazon EC2 даналары

Amazon Web Services қолдана отырып AMI негізінде жасалған виртуалды машина.

Amazon есептеуіш машинасының кескіні (AMI)

Виртуалды машинаны іске қосуға қажетті бағдарламалық жасақтаманың конфигурациясы бар үлгі. Бір AMI негізінде бірнеше даналарды жасауға болады.

AWS Application Program Interface (AWS API)

Kaspersky Security Center бағдарламасы пайдаланатын AWS платформасы қолданбасының бағдарламалық интерфейсі. AWS API құралдарымен, атап айтқанда, бұлттық сегменттерде сауалнама өткізу және даналарға Желілік агентті орнату жүргізіледі.

AWS IAM қатынас кілті

ID кілттен ("AKIAIOSFODNN7EXAMPLE" түрі) және құпия кілттен ("wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY" түрі) тұратын тіркесім. Жұп IAM пайдаланушысына тиесілі және AWS сервистерімен қатынасуды алу үшін пайдаланылады.

AWS басқару консолі

AWS-те ресурстарды қарауға және басқаруға арналған веб-интерфейс. AWS басқару консолі интернетте https://aws.amazon.com/ru/console/ бетінде қолжетімді.

Cloud Discovery

Cloud Discovery пайдаланушылардың бұлттық сервистерге қол жеткізуін басқарады. Бұлттық сервистерге, мысалы, Microsoft Teams, Salesforce, Microsoft Office 365 кіреді. Бұлттық сервистер санаттарға топтастырылған, мысалы, *Файлдармен алмасу*, *Мессенджерлер*, *Электрондық пошта*.

FileTransferBridge

Kaspersky қолданба жаңартуларын жергілікті жеткізуді қамтамасыз ететін Kaspersky Security Center Linux ішкі компоненті. FileTransferBridge Желілік агентке (klnagent) біріктірілген және әрбір басқарылатын құрылғыда жергілікті түрде жұмыс істейді.

Kaspersky қолданбалары Kaspersky Security Center Linux-тен жаңартуларды алған кезде, желілік агент жаңарту файлдарын Басқару серверден немесе тарату нүктесінен жүктейді. Содан кейін FileTransferBridge файлдарды жергілікті түрде орнатылған Kaspersky қолданбаларына тасымалдап, дерекқор жаңартулары мен бағдарламалық жасақтама патчтарының сенімді жеткізілуін қамтамасыз етеді.

FileTransferBridge 30522 және 30523 TCP порттарын пайдаланады. Порттар тек localhost (127.0.0.1) интерфейсінде жұмыс істейді және сыртқы желілерден кіріс қосылымдарды қабылдамайды.

HTTPS

Шифрлауды қолдана отырып шолғыш пен веб-сервер арасында деректерді жіберудің қауіпсіз протоколы. HTTPS корпоративтік немесе қаржылық деректер сияқты жабық ақпаратқа қатынасу үшін пайдаланылады.

IAM пайдаланушысы

AWS сервистерін пайдаланушы. IAM-пайдаланушы бұлттық сегменттерде сауалнама өткізу құқықтарына ие болуы мүмкін.

IAM рөлі

AWS сервистеріне сұрауларды орындауға арналған құқықтар жиынтығы. IAM рөлі ешқандай нақты пайдаланушыға немесе топқа байланысты емес және AWS IAM қатынас кілттерін пайдаланусыз қатынасу құқықтарын қамтамасыз етеді. IAM рөлін IAM пайдаланушысына, EC2 даналарына, AWS қолданбаларына немесе сервистеріне беруге болады.

Identity and Access Management (IAM)

Пайдаланушылардың AWS басқа сервистері мен ресурстарына қатынасын басқаруға көмектесетін AWS сервисі.

iOS MDM құрылғы

iOS MDM протоколы бойынша iOS MDM серверіне қосылатын ұялы құрылғы. iOS MDM протоколы бойынша iOS операциялық жүйесі бар құрылғылар қосылуы және басқарылуы мүмкін.

iOS MDM профилі

Басқару серверіне iOS ұялы құрылғыларын қосу параметрлерінің жиынтығы. Пайдаланушы ұялы құрылғыға iOS MDM профилін орнатады, содан кейін бұл ұялы құрылғы Басқару серверіне қосылады.

iOS MDM сервері

Клиент құрылғысына орнатылатын және iOS ұялы құрылғыларын Басқару серверіне қосуға және оларды Apple Push Notifications (APNs) сервисі көмегімен басқаруға мүмкіндік беретін Kaspersky Security Center құрамдасы.

JavaScript

Веб-беттердің мүмкіндіктерін кеңейтетін бағдарламалау тілі. JavaScript қолдана отырып жасалған веб-беттер веб-сервердегі деректермен веб-бетті жаңартусыз қосымша әрекеттерді орындауға (мысалы, интерфейс элементтерінің түрін өзгерту немесе қосымша терезелерді ашу) қабілетті. JavaScript, қолдана отырып жасалған веб-беттерді қарау үшін шолғыш параметрлерінде JavaScript қолдауды қосу керек.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network – бұл Kaspersky бағдарламалары орнатылған құрылғыларды пайдаланушыларға өз құрылғыларынан Kaspersky Security Network бағдарламасына деректерді жібермей, Kaspersky Security Network дерекқорларына және басқа да статистикалық деректерге қатынасуды қамтамасыз ететін шешім. Kaspersky Private Security Network келесі себептердің бірі бойынша Kaspersky Security Network бағдарламасына қатыса алмайтын ұйымдарға арналған:

- Құрылғылар интернетке қосылмаған.
- Кез келген деректерді елден немесе корпоративтік желіден (LAN) тыс жерге жіберуге заңмен немесе корпоративті қауіпсіздік саясаттарымен тыйым салынады.

Kaspersky Security Center System Health Validator (SHV)

Microsoft NAP-пен Kaspersky Security Center бағдарламасының бірлескен жұмысы кезінде операциялық жүйенің жұмысқа қабілетін тексеруге арналған Kaspersky Security Center бағдарламасының құрамдасы.

Kaspersky Security Center Web Server

Басқару серверінің құрамына орнатылатын Kaspersky Security Center құрамдасы. Веб-сервер жеке орнату пакеттерін, iOS MDM профильдерін, сондай-ақ ортақ қатынасы бар қалтадағы файлдарды желі арқылы беруге арналған.

Kaspersky Security Center әкімшісі

Kaspersky Security Center қашықтан орталықтандырылған басқару жүйесі арқылы бағдарламаның жұмысын басқаратын адам.

Kaspersky Security Center қолданбасын жаңарту

Осы қолданбаның бұрынғы нұсқасы орнатылған құрылғыға Kaspersky Security Center бағдарламасының жаңа нұсқасын орнату процедурасы.

Kaspersky Security Center операторы

Kaspersky Security Center көмегімен басқарылатын қорғаныс жүйесінің күйі мен жұмысын бақылайтын пайдаланушы.

Kaspersky Security Network (KSN)

Файлдардың, веб-ресурстардың және бағдарламалық жасақтаманың беделі туралы ақпаратты қамтитын Kaspersky тұрақты түрде жаңартылып тұратын дерекқорына қатынасуды қамтамасыз ететін бұлтты қызметтер инфрақұрылымы. Kaspersky Security Network Kaspersky бағдарламаларының қауіптерге реакциясының жоғары жылдамдығын қамтамасыз етеді, кейбір қорғаныс құрамдастарының тиімділігін арттырады, сондай-ақ жалған іске қосылудың ықтималдығын азайтады.

Kaspersky жаңарту серверлері

Kaspersky бағдарламаларына дерекқорлар мен модульдердің жаңартуларын жіберетін Kaspersky HTTP серверлері мен HTTPS серверлері.

KES құрылғылары

Басқару серверіне қосылатын және Kaspersky Endpoint Security for Android ұялы құрылғысы көмегімен басқарылатын ұялы құрылғы.

MITM шабуылы

Делдал шабуылы. Ұйымның АТ-инфрақұрылымына шабуыл, онда шабуылдаушы екі қатынас нүктесі арасындағы байланыс арнасын басып алады, оны ретрансляциялайды және қажет болса, осы қатынас нүктелері арасындағы қосылымды өзгертеді.

Network Location Awareness (NLA)

Операциялық жүйеге ағымдағы желіні анықтауға көмектесетін Windows қызметі. NLA желідегі өзгерістерді анықтайды және құрылғының қауіпсіздік конфигурациясын реттейді.

Provisioning профилі

iOS ұялы құрылғысында қолданбалардың жұмысына арналған параметрлер жиынтығы. Provisioning профилі лицензия туралы ақпаратты қамтиды және белгілі бір қолданбаға байланысты.

SSL

Жергілікті желілерде және интернетте деректерді шифрлау протоколы. SSL клиент пен сервер арасында қорғалған қосылыстарды жасау үшін веб-қолданбаларда қолданылады.

UEFI деңгейінде қорғанысы бар құрылғы

BIOS деңгейіне енгізілген UEFI үшін Kaspersky шешімі немесе бағдарламасы бар құрылғы. Кіріктірілген қорғаныс жүйені іске қосуды бастаған сәттен бастап құрылғының қауіпсіздігін қамтамасыз етеді, ал кіріктірілген БҚ жоқ құрылғылар қорғанысы тек қауіпсіздік бағдарламасы іске қосылғаннан кейін ғана әрекет ете бастайды.

Windows Server Update Services (WSUS)

Ұйым желісінде пайдаланушылардың құрылғыларында Microsoft бағдарламаларының жаңартуларын тарату үшін қолданылатын бағдарлама.

Антивирустық дерекқорлар

Антивирустық дерекқорларды шығарған сәтте Kaspersky белгілі компьютерлік қауіпсіздік қауіптері туралы ақпаратты қамтитын дерекқорлар. Антивирустық деректорлардағы енгізілімдер сканерленген нысандардан зиянды кодты анықтауға мүмкіндік береді. Антивирустық дерекқорларды Kaspersky мамандары жасайды және олар сағат сайын жаңарып отырады.

Антивирустық қорғаныс провайдері

Kaspersky шешімдері негізінде ұйым-клиенттің желілерінің антивирустық қорғаныс қызметтерін ұсынатын ұйым.

Арнайы құрылғыға арналған тапсырма

Ерікті басқару топтарынан арнайы клиент құрылғылары үшін анықталған және оларда орындалатын тапсырма.

Әкімшілік құқықтар

Exchange ұйымының ішінде Exchange нысандарын басқаруға арналған пайдаланушы құқықтары мен өкілеттіліктерінің деңгейі.

Әкімшінің жұмыс станциясы

Басқару консолі орнатылған немесе оны Kaspersky Security Center Web Console жұмыс істеу үшін қолданатын құрылғы. Бұл құрамдас Kaspersky Security Center басқару интерфейсі болып табылады.

Әкімші жұмыс станциясынан Kaspersky Security Center серверлік бөлігін басқарады. Әкімшінің жұмыс станциясын қолданып, әкімші Kaspersky бағдарламаларының дерекқорында қалыптастырылған ұйымның желісін орталықтандырылған қорғанысының жүйесін құрады.

Бағдарлама параметрлері

Оның тапсырмаларының барлық түрлері үшін ортақ және жалпы бағдарламаның жұмысы үшін жауапты бағдарлама жұмысының параметрлері: мысалы, бағдарлама өнімділігінің параметрлері, есептерді жүргізу параметрлері, сақтық қойманың параметрлері.

Бағдарламаларды орталықтандырылған басқару

Kaspersky Security Center ұсынатын басқару қызметтері көмегімен бағдарламаны қашықтан басқару.

Бағдарламаны тікелей басқару

Жергілікті интерфейс арқылы бағдарламаны басқару

Басқару консолі

Windows негізінде Kaspersky Security Center құрамдасы (бұдан әрі MMC негізіндегі Басқару консолі). Бұл құрамдас Басқару серверінің және Желілік агенттің басқару қызметтеріне қатысты реттелмелі интерфейс болып табылады.

Басқару плагині

Басқару консолі арқылы бағдарламаның жұмысын басқаруға арналған интерфейс болып табылатын мамандандырылған құрамдас. Әрбір бағдарламаның өз плагині бар. Ол Kaspersky Security Center көмегімен басқарылатын Kaspersky барлық бағдарламаларының құрамына кіреді.

Басқару сервері

Ұйым желісіне орнатылған Kaspersky бағдарламалары туралы ақпаратты орталықтандырылған сақтау функцияларын жүзеге асыратын Kaspersky Security Center бағдарламасының құрамдасы. Басқару сервері осы бағдарламаларды да басқара алады.

Басқару сервері деректерін сақтық көшірмелеу

Сақтық көшірмелеу утилитасы көмегімен жүргізілетін сақтық сақтауға және кейін қалпына келтіруге арналған Басқару серверінің деректерін көшірмелеу. Утилита мыналарды сақтауға көмектеседі:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері)
- Басқару топтарының құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат
- Қашықтан орнатуға арналған бағдарламалар дистрибутивтерінің қоймасы (Packages, Uninstall, Updates қалталарының мазмұны)
- Басқару сервері сертификаты

Басқару сервері сертификаты

Басқару сервері келесі мақсаттарда қолданатын сертификат:

- Microsoft Management Console (MMC) немесе Kaspersky Security Center Web Console консолі негізінде Басқару консоліне қосылған кезде Басқару серверінің түпнұсқалық растамасы;
- басқарылатын құрылғыларда Басқару серверінің Желілік агентпен қауіпсіз өзара әрекеттесуі;
- негізгі басқару сервері қосалқы басқару серверіне қосылған кезде басқару серверлерінің түпнұсқалық растамасы.

Сертификат автоматты түрде Басқару серверін орнатқан кезде жасалады, содан соң Басқару серверінде сақталады.

Басқару серверінің деректерін қалпына келтіру

Сақтық қоймаға сақталған ақпараттың негізінде сақтық көшірмелеу утилитасы көмегімен Басқару серверінің деректерін қалпына келтіру. Утилита мыналарды қалпына келтіруге көмектеседі:

- Басқару серверінің дерекқоры (оқиғаның Басқару серверінде сақталған саясаттар, тапсырмалар, бағдарлама параметрлері)
- Басқару топтарының құрылымы және клиент құрылғылары туралы конфигурациялық ақпарат

- Қашықтан орнатуға арналған бағдарламалар дистрибутивтерінің қоймасы (Packages, Uninstall, Updates қалталарының мазмұны)
- Басқару сервері сертификаты

Басқару серверінің клиенті (Клиент құрылғысы)

Желілік агент және Kaspersky басқарылатын бағдарламалары орнатылған құрылғы, сервер немесе жұмыс станциясы.

Басқару тобы

Орындалатын функцияларға және оларға орнатылатын Kaspersky бағдарламалар жиынтығына сәйкес біріктірілген арнайы құрылғылар. Құрылғылар оларды біртұтас құрылғы ретінде басқару ыңғайлылығы үшін топтастырылады. Топтың құрамына басқа топтар кіруі мүмкін. Топқа орнатылған әрбір бағдарлама үшін топтық саясаттар жасалуы және топтық тапсырмалар қалыптастырылуы мүмкін.

Басқарылатын құрылғылар

Басқару топтарының біріне қосылатын ұйым желісінің құрылғылары.

Белсенді кілт

Бағдарламаның жұмысы үшін ағымдағы сәтте қолданылатын кілт.

Бұлтты орта

Желіде біріктірілген бұлттық платформа негізіндегі виртуалды машиналар немесе басқа виртуалды ресурстар.

Виртуалды Басқару сервері

Ұйым-клиенттің желісін қорғау жүйесін басқаруға арналған Kaspersky Security Center бағдарламасының құрамдасы.

Виртуалды Басқару сервері қосалқы Басқару серверінің жеке жағдайы болып табылады және физикалық Басқару серверімен салыстырғанда келесі негізгі шектеулерге ие:

- Виртуалды Басқару сервері тек негізгі Басқару серверінің құрамында ғана жұмыс істей алады.
- Виртуалды басқару сервері жұмыс істеген кезде негізгі Басқару серверінің негізгі дерекқорын пайдаланады. Деректерді сақтық көшірмелеу және қалпына келтіру тапсырмаларына, сондай-ақ жаңартуларды тексеру және жүктеу тапсырмаларына виртуалды Басқару серверінде қолдау көрсетілмейді.
- Виртуалды сервер үшін қосалқы Басқару серверлерін (соның ішінде виртуалды) құруға қолдау көрсетілмейді.

Вирустық белсенділік шегі

Одан асып кету вирустық белсенділіктің және вирустық шабуыл қаупінің туындауы болып саналатын белгілі уақыт ішінде белгіленген типті оқиғалардың максималды рұқсат етілген оқиғалар саны. Бұл сипаттама вирустық эпидемиялар кезеңдерінде үлкен мәнге ие және әкімшіге вирустық шабуылдардың туындайтын қауіптеріне уақтылы әсер етуге көмектеседі.

Вирустық шабуыл

Құрылғыға вирус кіргізудің бірқатар мақсатты амалдары

Демилитаризацияланған аймақ (DMZ)

Демилитаризацияланған аймақ - бұл жаһандық желідегі сұрауларға жауап беретін серверлер орналасқан жергілікті желінің сегменті. Ұйымның жергілікті желісінің қауіпсіздігін қамтамасыз ету мақсатында демилитаризацияланған аймаққа қатынас шектелген және желілік экранмен қорғалған.

Жалпы сертификат

Пайдаланушының ұялы құрылғысын сәйкестендіруге арналған сертификат.

Жаңарту

Kaspersky жаңартулар серверінен алынатын жаңа файлдарды ауыстыру немесе қосу рәсімі (дерекқор немесе бағдарламалық модульдер).

Желілік агент

Нақты желілік түйінге орнатылған (жұмыс станциясы немесе сервер) Басқару сервері және Kaspersky бағдарламалары арасында өзара әрекеттесуді жүргізетін Kaspersky Security Center бағдарламасының құрамдасы. Бұл құрамдас Microsoft Windows жүйелері үшін әзірленген барлық бағдарламалар үшін бірыңғай болып табылады. UNIX операциялық жүйелері мен оларға ұқсас және macOS арналған Kaspersky бағдарламалары үшін Желілік агенттің бөлек нұсқалары бар.

Желінің антивирустық қорғанысы

Ұйым желісінің құрылғыларына вирустар мен спам жіберудің ықтималдығын азайтатын, желілік шабуылдар, фишинг пен басқа қауіптерді болдырмайтын техникалық және ұйымдық шаралар кешені. Антивирустық желі қорғанысы қауіпсіздік бағдарламалары мен сервистерін қолданған кезде, сондай-ақ ұйымда ақпараттық қауіпсіздік саясаты болған кезде және сақталған кезде артады.

Желінің қорғаныс күйі

Ұйым желісі құрылғыларының қорғалу дәрежесін сипаттайтын ағымдағы қорғаныс күйі. Желіні қорғау күйі желі құрылғыларында орнатылған қауіпсіздік бағдарламаларының болуы, лицензиялық кілттерді пайдалану, анықталған қауіптердің саны мен түрлері сияқты факторларды қамтиды.

Жеңіл N агенті (LWNGT)

Мобильдік құрылғыларда Kaspersky Endpoint Security-мен өзара әрекет протоколы. LWNGT (мобильдік протокол деп те аталады) мобильдік құрылғыларға желілік агентті орнатпай-ақ желілік агент ретінде жұмыс істейді.

Жергілікті тапсырма

Бөлек клиент компьютерінде анықталған және орындалатын тапсырма.

Жергілікті түрде орнату

Қауіпсіздік бағдарламасының дистрибутивінен орнатуды қолмен іске қосуды немесе құрылғыға алдын ала жүктелген жарияланған орнату пакетін қолмен іске қосуды көздейтін ұйым желісінің құрылғысына қауіпсіздік бағдарламасын орнату.

Ішкі пайдаланушылар

Ішкі пайдаланушы есептік жазбалары виртуалды Басқару серверлерімен жұмыс істеу үшін пайдаланылады. Kaspersky Security Center бағдарламасында ішкі пайдаланушылар шынайы пайдаланушы құқықтарына ие.

Ішкі пайдаланушы есептік жазбалары тек Kaspersky Security Center ішінде жасалады және пайдаланылады. Ішкі пайдаланушылар туралы мәліметтер операциялық жүйеге берілмейді. Ішкі пайдаланушылардың аутентификациясын Kaspersky Security Center жүзеге асырады.

Кеңінен таратын домен

Барлық түйіндері OSI (Open Systems Interconnection Basic Reference Model) желілік моделі деңгейінде кеңінен таратын арнаның көмегімен деректерді бір-біріне жібере алатын компьютерлік желінің логикалық учаскесі.

Кілт файлы

Сынақ немесе коммерциялық лицензия бойынша Kaspersky бағдарламасын қолдануға көмектесетін xxxxxxxx.key көру файлы.

Клиент әкімшісі

Ұйым-клиенттің антивирустық қорғанысын қамтамасыз етуге жауапты ұйым-клиенттің қызметкері.

Конфигурациялық профиль

iOS MDM ұялы құрылғылары үшін параметрлер мен шектеулер жиынтығын қамтитын саясат.

Күшпен орнату

Бағдарламалық жасақтаманы нақты клиент құрылғыларына қашықтан орнатуға мүмкіндік беретін Kaspersky бағдарламаларын қашықтан орнату әдісі. Күшпен орнату әдісімен тапсырманы сәтті орындау үшін тапсырманы іске қосуға арналған есептік жазба клиент құрылғыларында бағдарламаларды қашықтан іске қосу құқықтарына ие болуы тиіс. Бұл әдіс мұндай мүмкіндікке қолдау көрсетілетін Microsoft Windows операциялық жүйелерінің басқаруымен жұмыс істейтін құрылғыларға бағдарламаларды орнату үшін ұсынылады.

Қалпына келтіру

Нысан карантинге қоюға, емдеуге немесе жоюға дейін сақталған бастапқы орналасқан жерінің қалтасына немесе пайдаланушы көрсеткен басқа қалтаға түпнұсқа нысанды карантиннен немесе сақты қоймадан жылжыту.

Қашықтан орнату

Kaspersky Security Center бағдарламасы ұсынатын құралдар көмегімен Kaspersky бағдарламаларын орнату.

Қолданбалар дүкені

Kaspersky Security Center бағдарламасының құрамдасы. Қолданбалар дүкені пайдаланушылардың Android құрылғысына қолданбаларды орнату үшін пайдаланылады. Қолданбалар дүкенінде қолданбалардың apk-файлдарын және Google Play-де қолданбаларға сілтемелерді жариялауға болады.

Қолжетімді жаңарту

Құрамына белгілі кезеңде жиналған жедел жаңартулар жиынтығы және бағдарлама архитектурасындағы өзгерістер қосылған Kaspersky бағдарламалар модульдерінің жаңарту бумасы.

Қолмен орнату

Қауіпсіздік бағдарламасының дистрибутивінен ұйым желісінің құрылғысына қауіпсіздік бағдарламасын орнату. Қолмен орнату үшін әкімшінің немесе басқа IT-маманның тікелей қатысуы қажет. Кәдімгі орнату егер қашықтан орнату қатемен аяқталған пайдаланылады.

Қорғаныс күйі

Компьютердің қорғалу деңгейін сипаттайтын ағымдағы қорғаныс күйі.

Қорғанысты күшейту нұсқаулығы

Бұзылу қаупін азайту үшін Kaspersky Security Center және оның құрамдастарын конфигурациялаудың ұсыныстары мен ерекшеліктері.

Қосылым шлюзі

Қосылым шлюзі – ерекше режимде жұмыс істейтін Желілік агент. Қосылым шлюзі басқа Желілік агенттерінен қосылымдарды қабылдайды және оларды Сервермен орнатылған өзінің қосылымы арқылы Басқару серверіне туннельдейді. Әдеттегі Желілік агенттен айырмашылығы, қосылым шлюзі Басқару серверімен байланыс орнатпайды, тек Басқару серверінен қосылымдарды күтеді.

Қосымша (немесе резервтегі) лицензиялық кілт

Бағдарламаны қолдану құқығын растайтын, бірақ ағымдағы сәтте қолданылмайтын кілт.

Құрылғының иесі

Құрылғының иесі - бұл әкімші құрылғымен қандай да бір жұмыстарды орындау қажет болса байланысатын құрылғының пайдаланушысы.

Лицензия мерзімі

Сіз бағдарлама функцияларын және қосымша қызметтерді пайдалана алатын кезең. Қолжетімді функциялар мен қосымша қызметтер көлемі лицензияның түріне байланысты.

Лицензиялы бағдарламалар тобы

Клиент құрылғыларында олар үшін орнатудың есебі жүргізілетін әкімші белгілеген өлшемшарттар (мысалы, өндіруші бойынша) негізінде жасалған бағдарламалар тобы.

Оқиғалар қоймасы

Kaspersky Security Center-де туындайтын оқиғалар туралы ақпаратты сақтауға арналған Басқару серверінің дерекқорының бөлігі.

Оқиғаның маңыздылық деңгейі

Kaspersky бағдарламасының жұмысында бекітілген оқиғаның сипаттамасы. Келесі маңыздылық деңгейлері бар:

- Критикалық оқиға
- Функционалдық ақау
- Ескерту
- Ақпараттық хабар

Бірдей түрдегі оқиғалар оқиға орын алған жағдайға байланысты әртүрлі маңыздылық деңгейлеріне ие болуы мүмкін.

Орнату пакеті

Kaspersky Security Center қашықтан басқару жүйесімен Kaspersky бағдарламасын қашықтан орнату үшін қалыптастырылатын файлдар жиынтығы. Орнату пакеті бағдарламаны орнатуға және бірден орнатқаннан кейін оның жұмысқа қабілетін қамтамасыз етуге қажетті параметрлер жиынтығын қамтиды. Параметрлердің мәндері әдепкі бойынша бағдарлама параметрлерінің мәндеріне сәйкес келеді. Орнату пакеті бағдарлама дистрибутивінің құрамына кіретін kpd және kud кеңейтімдері бар файлдардың негізінде жасалады.

Осалдық

Зиянды бағдарламалық жасақтама өндірушілері операциялық жүйеге немесе бағдарламаға ену және оның тұтастығын бұзу үшін қолдана алатын операциялық жүйенің немесе бағдарламаның кемшілігі. Операциялық жүйедегі көптеген осалдықтар, оның жұмысын сенімсіз етеді, өйткені операциялық жүйеге енгізілген вирустар операциялық жүйенің өзінде де, орнатылған бағдарламаларда да ақаулық тудыруы мүмкін.

Патчтың маңыздылық деңгейі

Патчтың сипаттамасы. Үшінші тараптың немесе Microsoft патчтары үшін бес маңыздылық деңгейі бар:

- Критикалық
- Жоғары
- Орташа
- Төмен
- Белгісіз

Үшінші тараптың немесе Microsoft патчының маңыздылық деңгейі патч жабатын осалдықтың анағұрлым қолайсыз критикалық деңгейімен анықталады.

Провайдер әкімшісі

Антивирустық қорғаныс қызметтерінің провайдерінің қызметкері. Kaspersky шешімдері негізінде жасалған антивирустық қорғаныс жүйелерін орнату, пайдалану жұмыстарын орындайды, сондай-ақ клиенттерді техникалық қолдайды.

Сақтық көшірме қоймасы

Сақтық көшірмелеу утилитасы көмегімен жасалатын Басқару серверінің деректерінің көшірмелерін сақтауға арналған арнайы қалта.

Саясат

Саясат бағдарлама жұмысының параметрлерін және басқару тобының құрылғыларында орнатылған бағдарламаны конфигурациялауға қатынасты анықтайды. Әр бағдарлама үшін өз саясатын жасау қажет. Сіз әр басқару тобындағы құрылғыларға орнатылған бағдарламалар үшін көптеген саясаттар жасай аласыз, бірақ басқару тобының шегінде тек бір саясат бір уақытта әр бағдарламаға пайдаланылуы мүмкін.

Тапсырма

Kaspersky бағдарламасы орындайтын функциялар тапсырмалар түрінде іске асырылған, мысалы: Файлдарды нақты уақыт режимінде қорғау, Құрылғыны толықтай тексеру, дерекқорды жаңарту.

Тапсырма параметрлері

Әр тапсырма түрі үшін ерекше бағдарлама жұмысының параметрлері.

Тарату нүктесі

Жаңартуларды тарату, бағдарламаларды қашықтан орнату, басқару тобы және/немесе кеңінен таратылған доменнің құрамында құрылғылар туралы ақпаратты алу үшін пайдаланылатын Желілік агент орнатылған құрылғы. Тарату нүктелері жаңартуларды тарату кезінде және желідегі трафикті оңтайландыру үшін Басқару серверіне жүктемені азайтуға арналған. Тарату нүктелері автоматты түрде Басқару серверімен немесе қолмен әкімшімен тағайындалуы мүмкін. Тарату нүктесі бұрын жаңарту агенті деп аталды.

Топтық тапсырма

Басқару тобы үшін анықталған және осы басқару тобының құрамына кіретін барлық клиент құрылғыларында орындалатын тапсырма.

Түпнұсқалық растама агенті

Қатты жүктеу дискін шифрлаудан кейін шифрланған қатты дисктерге қатынасу үшін және операциялық жүйені жүктеу үшін түпнұсқалық растама рәсімінен өтуге көмектесетін интерфейс.

Үйдегі Басқару сервері

Үйдегі Басқару сервері – бұл Желілік агентті орнатқан кезде белгіленген Басқару сервері. Үйдегі Басқару сервері Желілік агентті қосу профильдерінің параметрлерінде пайдаланыла алады.

Үйлесімсіз бағдарлама

Үшінші тараптың антивирустық бағдарламасы немесе Kaspersky Security Center арқылы басқаруға қолдау көрсетпейтін Kaspersky бағдарламасы.

Ұялы құрылғылардың сервері

Ұялы құрылғыларға қатынасты ұсынатын және оларды Басқару консолі арқылы басқаруға мүмкіндік беретін Kaspersky Security Center құрамдасы.

Үшінші тарап коды туралы ақпарат

Үшінші тарап коды туралы ақпарат қолданбаны орнату қалтасындағы legal_notices.txt файлында бар.

Тауар белгілері туралы хабарландырулар

Тіркелген сауда белгілері мен қызмет белгілері - тиісті иелерінің жеке меншігі.

Adobe, Acrobat, Flash, Shockwave, PostScript – бұл Adobe компаниясының АҚШ-тағы және/немесе басқа елдердегі тіркелген сауда белгілері немесе сауда белгілері.

AMD, AMD64 – Advanced Micro Devices, Inc сауда белгілері немесе тіркелген сауда белгілері.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace – Amazon.com, Inc. немесе компанияның үлестес тұлғаларының сауда белгілері.

Apache – тіркелген тауар белгісі немесе Apache Software Foundation компаниясының АҚШ-тағы және (немесе) басқа елдердегі тауар белгісі.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID – Apple Inc. тауар белгілері.

Arm – АҚШ және/немесе басқа елдердегі Arm Limited (немесе оның еншілес компанияларының) тіркелген сауда белгісі.

Bluetooth ауызша тауар белгісі мен логосы Bluetooth SIG, Inc. компаниясына тиесілі.

Ubuntu, LTS – Canonical Ltd. компаниясының тіркелген тауар белгісі.

Cisco Systems, Cisco, Cisco Jabber, IOS – Cisco Systems, Inc. және/немесе оның үлестес компанияларының тауар белгілері немесе АҚШ-та және басқа елдерде тіркелген тауар белгілері.

Citrix, XenServer – Cloud Software Group, Inc. компаниясының және/немесе АҚШ-дағы және/немесе басқа елдердегі еншілес компаниялардың тіркелген сауда белгілері немесе сауда белгілері.

Corel – тауар белгісі немесе Канадада, Америка Құрама Штаттарында және басқа елдерде тіркелген Corel корпорациясының және/немесе оның еншілес компанияларының тауар белгісі.

Cloudflare, Cloudflare логотипі және Cloudflare Workers – Cloudflare, Inc. компаниясының сауда белгілері және/немесе АҚШ-та және басқа юрисдикцияларда тіркелген сауда белгілері.

Dropbox – Dropbox, Inc. тауар белгісі.

Radmin – Famatech компаниясының тіркелген тауар белгісі.

Firebird белгісі – Firebird қорының тіркелген тауар белгісі.

Foxit – Foxit корпорациясының тіркелген тауар белгісі.

FreeBSD белгісі – FreeBSD қорының тіркелген тауар белгісі.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS, YouTube – Google LLC тауар белгілері.

EulerOS, FusionCompute, FusionSphere – Huawei Technologies Co., Ltd. тауар белгілері.

Intel, Core, Xeon – Intel корпорациясының немесе оның еншілес компанияларының сауда белгілері.

IBM, QRadar – дүние жүзі бойынша көптеген юрисдикцияларда тіркелген International Business Machines Corporation тауар белгілері.

Node.js – Joyent, Inc. тауар белгісі.

Linux – АҚШ-та және басқа елдерде тіркелген Linus Torvalds тауар белгісі.

Logitech – тіркелген тауар белгісі немесе Logitech компаниясының АҚШ-тағы және (немесе) басқа елдердегі тауар белгісі.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista және Windows Azure – Microsoft компаниялар тобының тауар белгілері.

CVE – MITRE Corporation тіркелген тауар белгісі.

Mozilla, Firefox, Thunderbird – АҚШ-та және басқа елдерде тіркелген Mozilla Foundation тауар белгілері.

Novell – Америка Құрама Штаттарында және басқа елдерде тіркелген Novell Enterprises Inc. тауар белгісі.

NetWare – Америка Құрама Штаттарында және басқа елдерде тіркелген Novell Inc. тауар белгісі.

OpenVPN – OpenVPN, Inc. компаниясының тіркелген сауда белгісі.

OpenSSL – OpenSSL Software Foundation құқық иесінің тауар белгісі болып табылады.

Oracle, Java, JavaScript, TouchDown – Oracle Corporation және/немесе оның үлестес компанияларының тіркелген тауар белгілері.

Parallels, Parallels логотипі және Coherence – Parallels International GmbH компаниясының тауар белгілері немесе тіркелген тауар белгілері.

Chef – тауар белгісі немесе АҚШ-та және/немесе басқа елдерде тіркелген Progress Software Corporation және/немесе еншілес не үлестес компаниялардың бірінің тауар белгісі.

Puppet – тауар белгісі немесе Puppet, Inc. компаниясының тіркелген тауар белгісі.

Python – тауар белгісі немесе Python Software Foundation тіркелген тауар белгісі.

Red Hat, Fedora, Red Hat Enterprise Linux – Америка Құрама Штаттарында және басқа елдерде тіркелген Red Hat Inc. тауар белгілері.

Ansible – Red Hat, Inc. компаниясының АҚШ-та және басқа елдерде тіркелген тауар белгісі.

CentOS – Америка Құрама Штаттарында және басқа елдерде тіркелген Red Hat Inc. тауар белгісі.

BlackBerry тауар белгісі Research In Motion Limited компаниясына тиесілі, АҚШ-та тіркелген және басқа елдерде тіркеуге берілуі немесе тіркелуі мүмкін.

Rocky Linux – The Rocky Enterprise Software Foundation компаниясының сауда белгісі.

SAMSUNG – SAMSUNG компаниясының АҚШ-тағы немесе басқа елдердегі тауар белгісі.

Debian – Software in the Public Interest, Inc. тіркелген тауар белгісі.

Splunk, SPL – тауар белгілері және АҚШ-та және басқа елдерде тіркелген Splunk, Inc. сауда белгілері.

SUSE – АҚШ-та және басқа елдерде тіркелген SUSE LLC тауар белгісі.

Symbian тауар белгісінің иесі Symbian Foundation Ltd.

OpenAPI – Linux Foundation тауар белгісі.

UNIX – АҚШ-та және басқа елдерде тіркелген тауар белгісі, қолданылуы X/Open Company Limited тарапынан лицензияланған.

Zabbix – Zabbix SIA тіркелген тауар белгісі.

Шектеулер тізімі

Kaspersky Security Center Web Console сервері бағдарламаның жұмыс істеуі үшін критикалық емес бірқатар шектеулерге ие:

- 9838414: Microsoft Windows on Arm жүйесіне арналған желілік агентті жеке орнату пакетін пайдаланып орнату, құрылғы Әкімшілік серверге сәтті қосылған және орнату аяқталған болса да, **Басқару серверіне қосылым тексерілуде** қадамында қалуы мүмкін. Егер орнату осы қадамда жалғасса, орнату терезесін жаба аласыз. Microsoft Windows on Arm жүйесіне арналған Желілік агент бұрыннан орнатылған.

- 9978211: **Желілік агентті DMZ режимінде қосылым шлюзі ретінде пайдалану** опциясы Microsoft Windows жүйесінде Arm жүйесінде қолдау көрсетілмейді.

- Егер кестеде **Апта күндері бойынша** параметрі пайдаланылса, тапсырма кестесіне енгізілген өзгерістер басқарылатын құрылғыларға таратылмайды. Егер кестені жаңарту қажет болса, бар тапсырманы жойып, жаңартылған параметрлері бар жаңасын жасаңыз.

- Желілік агент Microsoft Windows XP жүйесінде орнатылған болса, басқарылатын Бағдарламаларды басқару компоненттері туралы ақпарат қолжетімді емес.

- Белсендіру кодын енгізу арқылы басқару серверінің қоймасына EDR Optimum кілтін қоссаңыз ғана, негізгі мәзірдің **Бақылау және есеп беру** бөлімінде консоль **Ескертулер** ішкі бөлімін көрсетеді.

- Криптографиялық күшті қамтамасыз ету үшін басқару серверінің сертификатына SHA-2 арқылы қол қойылуы және кілттің минималды ұзындығы 2048 болуы керек. Сертификатты қайта шығару қажет болса, Kaspersky Security Center білім қорын қараңыз.

- Kaspersky Security Center 15.1 Web Console ішіндегі **N күн сайын** және **Апта күндері бойынша** жоспарлау параметрлерімен тапсырма жасасаңыз, содан кейін тапсырманы Kaspersky Security Center Web Console немесе Kaspersky Security Center Administration Console алдыңғы нұсқаларымен ашсаңыз (мысалы, тапсырма Linux және Windows негізіндегі болуы мүмкін қосымша басқару серверлерінде де қолданылса), жоспарлау параметрлері дұрыс көрсетілмеуі немесе қате пайда болуы мүмкін.

- Kaspersky Security Center Web Console-де SIEM жүйелеріне экспорттауды конфигурациялағанда және UDP протоколын таңдаған кезде, **Байланысты тексеру** түймесін басқаннан кейін, қате пайда болады, себебі UDP байланыс орнатпайды және деректерді жеткізуге кепілдік берілмейді.

- Arm архитектурасына негізделген және Astra Linux Special Edition RUSB.10015-01 (кезекті жаңарту 1.7) негізінде жұмыс істейтін құрылғыда Желілік агентті жою тапсырмасын іске қосқанда, Желілік агент сәтті жойылады, бірақ тапсырмалар тізіміндегі ағымдағы прогресс үшін тапсырма күйі қатып қалды.

- Exchange ActiveSync-ке бұдан былай қолдау көрсетілмегенімен, Kaspersky Device Management for iOS сипаттары терезесі әлі де **EAS құрылғылары параметрлері** бөлімін қамтиды.

- Kaspersky Security Center құрылғы атауында кириллица таңбалары бар құрылғыда орнатылған болса және KSN прокси-сервері Басару серверінде қосылған болса, KSN желісіне HTTPS арқылы қосылу сәтсіз аяқталады.

- Сіз **Пайдаланушы есептік жазбасын өзгерту рұқсатын тексеру үшін аутентификацияны сұрау** параметрі қосылған пайдаланушы есептік жазбасының сипаттарын өзгертуге тырысқанда, содан кейін **Есептік жазба қорғанысы** терезесіндегі **Бас тарту** түймесін басқанда, күтпеген қате орын алады.

- Құрылғыдағы уақытты немесе уақыт белдеуін өзгертсеңіз, Kaspersky Security Center Web Console қызметін қайта іске қосуыңыз керек.

- Құрылғыда прокси-сервер пайдаланылса және прокси-сервер ортасының айнымалы мәндері орнатылса, Kaspersky Security Center Web Console орнату бағдарламасы қатып қалуы мүмкін.

- *Тарату нүктелерінің қоймасыға жаңартуларды жүктеп алу* немесе *Жаңартуларды тексеру* тапсырмасын импортталған кезде, **Тапсырма тағайындалатын құрылғыларды таңдау** параметрі қосулы болады. Бұл тапсырмаларды құрылғы таңдауларына немесе бекітілген құрылғыларға тағайындау мүмкін емес. *Тарату нүктелерінің қоймасыға жаңартуларды жүктеп алу* немесе *Жаңартуларды тексеру* тапсырмасын белгілі бір құрылғыларға тағайындасаңыз, тапсырма дұрыс импортталмайды.

- Желілік агенттің 15-нұсқасы орнатылған Linux операциялық жүйесімен жұмыс істейтін тарату нүктесін пайдалансаңыз, мекенжай мен пайдаланушының есептік жазба деректерін көрсеткен Active Directory домендеріне ғана сауалнама жүргізуге болады. Ағымдағы Active Directory домені мен Active Directory доменінің тобы үшін сауалнама жүргізу қолжетімді емес.

- Windows желі сауалнамасын бастағаннан кейін, клиент құрылғылары табылмауы мүмкін.

- Болашақ қосалқы Серверде, **Қосалқы Басқару серверін қосу** шебері терезесінде түпнұсқалық растама үшін екі қадамдық тексеруы қосылған есептік жазбаны көрсетсеңіз, шебер өз жұмысын қатемен аяқтайды. Бұл мәселені шешу үшін, екі қадамдық тексеруі өшірілген есептік жазбаны көрсетіңіз немесе болашақ қосалқы Серверден иерархия жасаңыз.

- Kaspersky Security Center Web Console серверіне кірген кезде, сіз домендік түпнұсқалық растаманы қолдансаңыз және қосылу үшін виртуалды Басқару серверін көрсетсеңіз, содан соң бағдарламадан шығып, негізгі Басқару серверіне кіруге тырыссаңыз, онда Kaspersky Security Center Web Console сервері әлі де болса виртуалды Басқару серверіне қосылады. Негізгі Басқару серверіне қосылу үшін браузерді қайта ашыңыз.

- Windows желісінің жылдам/толық сауалнамасы бос нәтижені қайтарады.

- Kaspersky Security Center Web Console серверін Есептік деректер және қатынасу диспетчерімен бірге орнатсаңыз, содан соң Kaspersky Security Center Web Console Басқару серверін ауыстырсаңыз, Есептік деректер және қатынасу диспетчері құрамдасы жаңа Басқару сервері туралы ақпаратты алмайды.

- Бірнеше желілік адаптері бар басқарылатын құрылғы Басқару серверіне қосылу үшін пайдаланылатын желілік адаптерден ерекшеленетін желілік адаптердің MAC мекенжайы туралы ақпаратты Басқару серверіне жібереді.

- CEF деректер форматы таңдалған кезде, SIEM жүйесіне арналған сынақ қосылымы сәтсіз аяқталады.

- NTLM аутентификациясы Қорғалған пайдаланушылар тобындағы пайдаланушы есептік жазбалары үшін жұмыс істемейді.